RECOMMENDATIONS FOR "PAYMENT ACCOUNT ACCESS" SERVICES DRAFT DOCUMENT FOR PUBLIC CONSULTATION

Comments of SOFORT AG, Gauting, Germany

Dear Sirs,

Thank you for the invitation to comment on the draft recommendations for "payment account access services" (in the following "**recommendations**"). We appreciate the open consultation with all parties concerned and the fact that the recommendations recognize the fact that "payment account access services" ("**PAAS**") have become part of everyday business, rapidly gaining importance notably in e-commerce. Furthermore, we believe that defining common standards will help to protect market access notably for bank-independent services, creating a level playing field throughout the Union.

Nevertheless, in the following, we will provide some comments, following the structure of the recommendations.

Introduction

(1) We believe that the recommendations still **discriminate** against bank-independent Payment Initiation Services ("**PIS**")[1], because the recommendations exclude (i) locally installed software that operates via the internet as well as (ii) products offered by account servicing banks (or their subsidiaries[2]). Under the current recommendations, neither of them would have to abide by the same standards and rules as applicable for bank-independent PIS, which would distort competition and hinder the creating of a level playing field.

The position was different in the ECB's 7th progress report, page 30, where "online e-payments" had been defined as any payment *"for which the payment data and the payment instruction are transmitted and confirmed online (i.e. via the internet) between the customer and his/ her payment service provider"*. On page 29 he report said: *"No differentiation is made between the device (desktop PC, laptop, netbook, mobile handsets) and/or the service technology used to access the internet. As long as the payment data is transmitted and confirmed via the internet, it is considered as an online e-payment"*.

[1] Sofort AG provides a so-called Payment Messenger Service ("**PMS**") that can be used to initiate payments via the internet (therefore constituting a PIS) and that, additionally, sends an instant payment confirmation to the merchant (hence " messenger").

[2] These companies are often not regulated.

Accordingly, in our view, the definition of PIS should be

> *"the provision of software and related services to payment account holders, designed to enable payment account holders to access their payment accounts via the internet and initiate payments from their payment account".*

On that basis, the restriction of the recommendations to "third party service providers" ("**TPs**") should be abandoned to include all PAAS (PIS and account information services ("**AIS**")) active in the market, regardless of whether it is being offered by the account-servicing PSP or not. Furthermore, so-called governance authorities ("**GAs**") should always be subject to the same rules as PIS/PAAS.

By the same token, third-party service providers ("**TPs**") and governance authorities ("**GAs**") should always be subject to the same rules.

(2) The recommendations sometimes may risk to create **new barriers to entry** by imposing far-reaching amendments to the business models in question. For example, when discussing prior registration of customers and authentication (recommendation 7) or enrolment (recommendation 8), it should be made clear that these recommendations only apply to PAAS that use prior registration and enrolment, but that the recommendations do not impose on all PAAS a duty of enrolment and prior registration. Another example is the initial customer identification (recommendation 6), where it should be made clear that the recommendations request identification in compliance with anti-money laundering legislation, but that the recommendations do not impose identification in excess of these legal requirements.

The above issues mainly arise in the context of the brackets stating "where applicable" (e.g. recommendations 6, 7, 8, 9). Accordingly, for the sake of clarity, the recommendations should make clear where its rules are not meant to apply.

In particular, if recommendation 7 was not clearly limited to *"TPs requiring prior registration"*, recommendation 7.1 KC could be interpreted as a duty to set up a second authentication for all PAAS, also for ad-hoc services that currently do not use prior registration. However, such second authentication would be redundant and pointless, not enhancing security but creating a prohibitive burden for services that rely on a-hoc availability without prior registration. It would effectively eliminate an entire business model.

The same applies for prior identification, which would again disable ad-hoc services that rely on ad-hoc availability. Therefore, to the extent anti-money laundering provisions do not impose identification, or provide for exemptions (e.g. where the service does not hold funds, which applies for PIS), the recommendations should not impose identification in excess of anti-money laundering provisions. Otherwise, the recommendations would, again, disable an entire business model.

Moreover, if the discriminatory distinction between bank-independent PIS on the one hand, and bank-owned services and/or software on the other, was upheld (see point 1, above), only bank-independent services would become subject to such over-reaching obligations, creating a strong competitive disadvantage that would distort competition in favour of the banking industry.

(3) To avoid potential overregulation and/or market distortion, another explicit guiding principle of the recommendations should be to open markets, enable services and create a level playing field. On that basis, the recommendations should not exclude or prefer certain business models, and should refrain from imposing obligations that are unnecessary or disproportionate. This coincides with the ECB's neutrality as well as the protection of the fundamental freedom to provide services within the Union.

In this context, the recommendations should acknowledge that the core problem with PAAS has been the conflict of interest of banks and the abusive obstruction of bank-independent PIS. In practice, the problem with PIS has not been security or data protection, but above all illegal and anticompetitive obstruction by market incumbents. One explicit aim of the recommendations therefore should be to protect market entry and free competition. Therefore it should be made clear that the recommendations should be interpreted in a way that they aim to support a high level of security, but also to foster competition and open the market for bank-owned as well as bank-independent companies.

(4) Against this background, we believe the following core principles should be added to the guiding principles of the recommendations:

(i) **Equal Treatment**: The recommendations must not discriminate against a particular kind of service, and must follow the principle of equal treatment.

Accordingly, bank-owned services and bank-sponsored joint ventures as well as software applications designed to access the payment account via the internet, regardless of the end-device being used or the place of storage, should be subject to the same recommendations.

(ii) **Proportionality:** The recommendations need to remain neutral, avoiding to distort competition and limiting restrictions to what is necessary and proportionate to protect public interests. The recommendations therefore should avoid overregulation..

(iii) **Protection of Market Access and Level Playing Field:** The recommendations should protect market access against abusive practices by incumbent market players.

The recommendations should acknowledge the problem of abusive obstruction by the financial industry, which has led to several antitrust proceedings (*inter alia*, against the EPC) and the current debate to regulate PAAS. On that basis, the recommendations should declare the aim of creating a level playing field, where secure PAAS can be used and must not be restricted by account servicing PSPs.

(5) In particular, Payment Messenger Services ("**PMS**")[3] are currently one of the safest ways for consumers to pay online. PMS have performed outstandingly, providing a level of security and reliability higher than for traditional payment methods such as, *e.g.*, credit cards, which suffer from high fraud rates and low security ratings and which are (not least due to a lack of competition) very expensive. It is widely acknowledged also within the banking industry that PMS provide additional security, efficiency and competition to merchants and consumers.

The problem is that account servicing banks have abused their powers under the Payment Services Directive ("**PSD**") to stop the use of bank-independent PMS in order to control prices and reserve business for themselves.

The aim of the recommendations therefore should be to support the on-going process of harmonisation of standards for PMS in order to open markets, as banks must not be allowed to use security as a pretext. As Vice-President Almunia put it (Speech 12-325): *"What counts is that safety and other standards are not used as a pretext to hinder competition and block innovative products."*

In reaction to past malpractice, the aim should be to create a level playing field that guarantees market access. As Vice-President Almunia put it (Speech 12-325): *"Ensuring a level playing field among existing providers of payment services and new entrants is also a key element in an antitrust investigation we opened against the EPC last September. We want to make sure that certain standards used for internet payments – based on those used in home-banking – do not discriminate against players that are not controlled by a bank."*

(6) In the following, we provide more detailed comments on selected passages of the recommendations. The core issues are:

(a) Respect the limitations of data protection legislation with regard to traceability (recommendation 5).

[3] A form of PIS, where the account holder, in addition to initiating payments, sends a payment confirmation to his seller. Sofort AG offers the PMS service Sofort Banking.

(b) Do not impose a duty of prior identification of users, where money laundering legislation does impose that duty; do not impose duty to have framework contracts (both recommendation 6).

(c) Clarify that there is no duty of prior registration; and clarify that duty of additional authentication only applies to services that use prior registration (both recommendation 7).

(d) Clarify that there is no duty of customer enrolment (recommendation 8).

(e) Ensure strict equal treatment of TPs, software, GAs and bank-owned software / services (all recommendations; definition of "Payment Initiation Service").

(f) Do not impose or create duties in excess of applicable data protection legislation (recommendation 11).

(g) Do not impose technical specifics that would lead to an overregulation and indirectly disable the business model of ad-hoc services, e.g. the requirement to set individual limits that would force to offer individual accounts (recommendation 13) or the requirement to inform on the status of the transaction for PIS that do not have this information (recommendation 14), while at the same time both pieces of information are easily accessible for the consumer by using his/her online-banking account.

(h) Correct and sensible definition of "sensitive payment data" (glossary)

I GENERAL PART

(1) The recommendations rely to a large extent on the previous recommendations for the security of internet payments. However, it should be kept in mind that PAAS generally do not handle funds. This is why they are currently not regulated under the PSD. Accordingly, requirements that have been imposed on payment service providers because they hold funds, run accounts and execute payments should not be transposed to multibank software services that do not hold the funds.

This applies, *inter alia*, to money laundering legislation (recommendation 6.1 KC) that often do not apply to PIS or other PAAS. Accordingly, the recommendations should not impose these rules in excess of legal requirements.

The same applies for imposing limits (recommendation 13) or the provision of information on the status of the transaction (recommendation 14). Both stem from the "internet recommendations" and originally refer to PSPs that run accounts and hold funds. Ad-hoc PIS, however, that do not register customers and do not run accounts, cannot provide for individualized limits. And generally, PIS cannot confirm the execution of the payment, which is not executed by them.

(2) The recommendations are supposed to apply to *"TPs providing payment account access Services for accounts they have not issued themselves"*. Accordingly, services offered by the account holding banks (mono-bank solutions and/or multibank services) would not have to abide by the same rules and standards as bank-independent services. We cannot see a reason for this privilege as these services offer the same services based on the same technologies.

For example, the recommendations require traceability, monitoring, data minimization and checks of e-merchants. Why should bank-owned service providers not be subject to these rules? They are providing the same service or software, and there is no difference with regard to the perceived risks. Hence, the rules have to apply equally. Otherwise, if there was a special regime for non-bank multibank software services, competition was distorted and the EU would fail its aim to create a level playing field, with bank-products suddenly being subject to lower standards.

The same applies for "governance authorities" ("**GAs**") that manage a joint multibank software service provided by account holding banks. Why should a cooperative multibank service owned by banks be treated different from a bank-independent service offering the same service?

A privilege for bank-owned multibank software services would create a market dominated by joint bank solutions (similar to the imposition of the so-called "four corner" or contract model, as previously proposed by the EPC). From an antirust perspective, this engenders the risk of anticompetitive coordination between the owning banks. As an example, the Dutch NMa and the German FCO raised antitrust concerns with regard to the joint pricing for the collectively owned multibank software services iDEAL and giropay. Further, due to the network effects in payment markets, collective solutions would need to include virtually all banks, which created an incentive for collective monopolies (or duopolies, as for credit cards). These problems do not arise with bank-independent services, which therefore should not be discriminated against but protected against obstruction by market incumbents to ensure competition (see guiding principle (iii), above). This is in the interest of consumers and also helps to create a Single Euro Payments Market beyond isolated national solutions.

Accordingly, to ensure **equal treatment** (see core principle (i) above), we propose to apply the recommendations to all services and software products that enable access the payment account via the internet. The restriction to "TPs" should be abandoned entirely, and the definition of PIS should be:

> *"the provision of software and related services to payment account holders, designed to enable payment account holders to access their payment accounts via the internet and initiate payments from their payment account"*.

This also needs to include "software applications", as referred to in footnote 6 of the recommendations ,that may or may not be installed locally on consumer end-devices, but that in any event connect to the bank account and transfer data via the internet. Therefore, any software or service that connects to the account via the internet should be defined as "internet-based".

Locally installed software does not use different technologies and does not offer security advantages. To the contrary, locally installed software (e.g. smartphone apps, home-banking, aggregation software) generally is more vulnerable, as consumer end-devices are hardly protected as comprehensively and professionally as central web-servers (*e.g.*, giropay web-servers). This is the main reason why PMS usually are hosted centrally on one web-server. However, this should not lead to the result that local software is subject to different, let alone less stringent standards.

In its 7th progress report, the ECB advocated this principle of equal treatment, see page 29: *"No differentiation is made between the device (desktop PC, laptop, netbook, mobile handsets) and/or the service technology used to access the internet. As long as the payment data is transmitted and confirmed via the internet, it is considered as an online e-payment and not an m-payment."*

(3) We agree that "account information services" ("**AIS**") also need to be included, as they use the same multibank technologies. Again this should be based on a broader definition that covers all AIS that connect to the account over the internet, regardless of the place of storage Most AIS enable to initiate payments anyway. In that case, they should be subject to the rules applicable to PIS (as defined above).

As a result, the recommendations should apply to all PIS and AIS (PAAS), regardless of whether they are bank-owned or not, and regardless of where the respective software is being stored. The limitation to "TPs" should be abandoned altogether.

OBJECTIVE OF THE RECOMMENDATIONS

(1) The recommendations require *"traceability through proper authentication in all Communications between the entities involved (i.e. the TP, the account servicing PSP, the e-merchant and the account owner)"*

When using multibank software services, the account holder communicates with his bank via the software provided by the service provider. He uses the software to identify and authenticate himself. Accordingly, the software provider has immediate feedback if that identification/authentication would fail, providing a reliable basis to identify and authenticate the customer. If the customers identifies and authenticates successfully towards his bank, he also does so automatically towards the software provider. A separate or additional identification/authentication towards the software provider would therefore be redundant. Moreover, it would be pointless, as the transaction can only be initiated if the user identifies and authenticates towards the bank that holds the funds to be transferred.

Accordingly, PIS should not be imposed a duty to provide separate authentication, at least to the extent that they do not request prior registration of account owners (cf. recommendation 7 and guiding principles, below).

(2) The recommendations require that *"TPs entering into contractual agreements with e-merchants should ensure that the e-merchants comply with the necessary security requirements"*.

We agree that multibank software service providers should monitor and select e- merchants, which SOFORT already does. As set out before, this should also apply to bank-products and local software applications (see guiding principle (i), above). It would be absurd if bank-owned services were subject to lesser standards, gaining a competitive advantage based on less security.

Accordingly, not only "TPs" but all PIS (as defined above) should be subject to the above rule.

SCOPE AND ADDRESSEES

(1) It is unclear how *„internet-based"* should be defined. As set out above, to ensure equal treatment and a level playing field, it should be defined to include any multibank software or service that connects to the account via the internet, irrespective of the device or location of storage (cf. 7th progress report, pages 29/30).

(2) The recommendations *"exclude traditional online payments and/or the supply of account information without the involvement of a third-party service provider"*.

As set out above, we believe that any software or service that enables to access accounts via the internet should be included. Therefore, also "traditional online payments" and/or services offered by banks should be included if they are designed to enabling accessing the payment account via the internet. In other words, the recommendations should not be limited to "TP"s as defined in the glossary, but should apply to all PIS and AIS on the basis of the above definition. There is no reason to create a different set of rules depending on who offers the software or service. The limitation to "TPs" should be abandoned altogether.

PMS have triggered the discussion of multibank software services, because they are subject to discriminatory obstruction. The solution to that conflict is the strict application of the principle of equal treatment, notably with regard to bank-owned products. If equal treatment was ensured, arbitrary obstruction would become very difficult.

(3) The recommendations exclude *"mobile payments other than browser-based payments"* and adds that *"specific recommendations applying to the release and maintenance of Software applications will be die subject of a separate work stream on mobile payments."*

Other software products that enable to access the account and initiate payments via the internet (see above definition of PIS) should also be included, regardless of whether they are "browser-based". In particular, if the software is installed locally (e.g., smart-phone apps or local home-banking software), it should also be included, because they use the same kind of software and technology and the only difference is the place of storage (cf. ECB 7th progress report, pages 29/30).

GUIDING PRINCIPLES

(1) We welcome that the recommendations allow for future developments in that they do not impose technical details, which would risk to create a straightjacket. Nevertheless, as set out above, we believe that three core guiding principles should be added: (i) equal treatment, (ii) neutrality and (iii) protection of market access.

With regard to the principle of *"strong authentication in case of prior registration"*, it is important to stress that this is limited to PAAS that use prior registration. Many multibank software services do not register users, which is a core part of their business model offering ad-hoc services. They rely on the fact that users have to be registered with the account holding PSP. This suffices to attain a high level of security. A second registration with the multibank software service provider would be redundant and pointless in that it could not create additional security with regard to the transaction that is, after all, being executed by the account servicing PSP.

(2) We agree that data protection legislation is in place and should not be circumvented by the recommendations. Hence, a service that is legal under data protection law, should not be described as illegitimate under the recommendations.

II RECOMMENDATIONS

4.1 **KC**	**Undermining of IT security**	It would be important to define what is meant by “undermining”. Banks have often claimed that forwarding their security credentials via software would “undermine” their security. However, when challenged to explain what such “undermining” was supposed to be, they cannot show increased security risks that would justify a prohibition of using multibank software services. To the contrary, PMS have proven that they currently one of the safest way to pay online and in practice do not lead to additional security risks. Therefore, following the guiding principle (iii) above, the recommendations should avoid using general terms that lend themselves for abuse. The claim that using secure and certified services still would “undermine” security needs to be excluded. To achieve this, instead of “undermining” the rule could be that: *“TPs and GAs should have appropriate security and control measures in place to ensure that their systems cannot be abused or manipulated for fraudulent abuse to the detriment of account holders or banks.”*

4.9 **KC**	**Arbitrary distinction of GAs**	4.9 KC provides a vivid example for the arbitrary distinction between “GAs” and “TPs”. While “TPs” (i.e. bank-independent service providers) must not authorise-merchants to handle sensitive payment data, GAs (bank-owned joint ventures) are free to do so. There is no reason why GAs should not abide by the same rule. Further, the definition of „handling sensitive data“ should not exclude e-merchants from handling payment data unrelated to the use of payment initiation software services. For example, for offering direct debit, merchants need to handle customers’ account data. Further, data that the merchant receives in any event (e.g. on his bank statement) should not be handled as “sensitive” as they are not confidential (*e.g.*, the buyer’s account number and sort code). See also comment on the definition of “sensitive payment data”.

4.10 **KC**	**Referral to internet recommendations**	The broad referral to the “internet recommendations” is too vague. The Internet recommendations refer to PSPs that hold funds, and contain many rules that apply because of holding and handling funds. In contrast, multibank software services do not hold funds or execute payments but can only be used to initiate payments. Therefore, many

		rules of the internet recommendations cannot apply “mutatis mutandis”. There was a good reason why the recommendations for PAAS have been separated from the internet recommendations, Accordingly, it would be contradictory if the internet recommendations became effective in total for all PIS. Such a broad reference to the “internet recommendations” would undermine legal certainty.

5	**Traceability and data protection**	Traceability needs to respect the limits of data protection legislation. For example, SOFORT is obliged by data protection law to limit the checks of its software to what is necessary to deliver the service mandated by the customer / account holder (“need-to-know-principle”). The ECB requires in section 4.5 KC that use and storage of data *“should be kept at the absolute minimum level”* (data minimisation). In section 11.4 KC the ECB refers to the *“proportionality principle”*. Accordingly, the recommendations should explicitly confirm that data protection laws need to be respected and should check whether the broad demands with regard to tracing and log files could be reconciled with data protection. In any case, under the “comply or explain” rule, service providers should have a valid justification for less traceability in case data protection authorities opposed certain measures. In addition, it could be laid down that prevention of fraud is a legitimate interest that may justify storage of data in some cases within the limits of data protection laws.

5.5 KC	**Identification towards PSP**	With regard to account servicing PSPs it must be assured that the latter do not abuse identification of the multibank software services in order to block or obstruct independent services. This is what they have been threatening for years. Accordingly, the recommendations first of all would need to ensure market access and enforce the principle that secure services must not be obstructed, see guiding principle (iii), above. As an example, Dutch banks jointly took the position that account holders must not use bank-independent PMS. They claimed that bank customers, via banks’ terms and conditions, have been prohibited to use security credentials in order to use other services than the banks’ joint service, iDEAL. German banks took a similar stance, triggering

		the antitrust proceedings in Germany. If this position was upheld, identification towards the account servicing PSPs would lead to the implementation of a boycott foreclosing the market to bank-independent competitors. As a general note, this shows that it is necessary to recognize the full extent of problems raised by the obstruction and market foreclosure by the incumbent account holding PSPs. These illegal activities triggered antitrust proceedings as well as the debate of regulating PMS under the PSD. The recommendations should acknowledge the ongoing abuse and commit banks to accept secure services. This would lead to the rule that banks must not abuse the authentication for obstruction and must not arbitrarily withhold or restrict access on that basis.

5.5 KC	**Identification towards PSP**	Same point as 5.5 KC, above. A "distinction" must not lead to discrimination, i.e. access must not be restricted or obstructed for PIS. Again, the prerequisite would be that the ECB enforces a strict principle of equal treatment (guiding principle (i), above), prohibiting to obstruct independent services (guiding principle (iii), above). We would therefore propose to amend 5.6 KC by saying *", while this must not be used for discrimination of PAAS or obstruction of access when using PAAS"*

5.1 BP	**Specific credentials for PAAS**	It would substantially restrict market access if such alternative authentication would allow banks to prohibit the use of ordinary credentials for multibank software services. The ease of use relies to a large extent on the fact that the account holder can use his ordinary procedure. Therefore, according to the guiding principle (iii), above, the rule should be that banks must not restrict the use of ordinary credentials. The identification of the multibank software service does not require a special authentication. Instead, as set out above, identification of the service, which is already required in 5.6, would not be a problem as soon as banks refrained from unfair obstruction. Thus, based on the principle of proportionality (guiding principle (ii), above) it is less burdensome and more pro-competitive to fight obstruction in the first place, which would allow identification, instead of creating a special regime that reinforces obstruction.

		5.1 BP should therefore be deleted.

6	**Customer identify-cation**	It appears that the recommendations rely on the model of its "internet recommendations", even though the latter refer to a different kind of service. Payment service providers hold funds and conclude framework agreements. They also enroll and register customers and, above all, fall under money laundering legislation, which obliges them to identify each customer. This is not the case for many PAAS.

6.1 **KC**	**Customer identify-cation**	What does „where applicable" refer to? It should mean that the sweeping obligations to identify customers should only apply where legislation imposes it. This is not the case for most PIS and many other PAAS: Money laundering provisions do not apply, to PIS that neither hold funds or accounts nor execute the transaction. If all PAAS were imposed a duty of initial identification, this would effectively exclude the business model of ad-hoc services, as this would mean that for any ad-hoc transaction, identification procedures would need to be completed. For example, PMS are available ad-hoc without registration or identification. If identification was imposed, PMS would have to introduce individualized accounts for any customer, creating new risks and data, excluding any spontaneous ad-hoc use. PMS providers would find it virtually impossible to subject software users to a full identity check before using the software. Above all, there is no reason to do so, which is why anti money laundering provisions do not apply. To the contrary, creating virtual accounts could engender new risks, which should be avoided. In addition, when using PMS the user has to identify himself to his bank before he can open his account. As using PAAS is just another form of using the payment account, identification is already being assured. The money is transferred from one bank account, where the consumer is already identified and which is under full control of the oversight authorities, to another bank account, where the merchant is already identified and which is under full control of the oversight authorities. In contrast, imposing a separate duty to identify without an account would be redundant and pointless. Adhering to the principle of proportionality (see guiding principle (ii) above), the recommendations must not impose pointless rules that restrict the provision of services and eliminate an entire business model (i.e. ad-

		hoc services). Accordingly, the recommendations should make clear that the above statement is limited to cases where anti money laundering legislation applies. In any case, it should not apply if the PIS or AIS has no customer account, but exclusively provides its services “ad-hoc”. In this context, footnote 17 should be amended as follows to define “where applicable”: *“The customer identification process is without prejudice to any exemptions provided in existing anti-money laundering legislation. Thus, PAAS need not conduct a separate customer identification process, if (i) such customer identification has already been carried out, e.g. for other existing services, or (ii) anti-money laundering legislation does not apply.”*

6.2 **KC**	**Information**	Under the current PSD, it is sufficient to “make” relevant information “available”. The term “supply” as used in the recommendations could be interpreted as meaning actual provision or active sending. This would be a far-reaching administrative burden. The term should therefore be defined in correspondence with the PSD as “provide or make available”.

6.3 **KC**	**Framework contract**	It should be clear that there is no duty to have a framework contract. The current business model of PMS and other multibank software services relies on case-by-case use, without framework contracts, enrolment, registration etc. (see above). There is no advantage in excluding these ad-hoc contractual relationships. Quite the contrary, the ad-hoc use is the cornerstone of the very successful security and data minimization policy applied by PMS.

6.1 **BP**	**Framework contract**	This must not lead to a duty to „sign“ a contract before any ad-hoc use of ready-to-use software services. The term “sign” does not fit into the online-world. Usually, there is no “general service contract”, as the use is on an ad-hoc basis.

7	**Prior registration**	PMS and most other access service providers do not *“require prior registration”* of account holders using PMS. The ad-hoc ability to use their software/services is a core part of the business model as well as of the security strategy.

		Accordingly, recommendation 7 does not apply, if PAAS do not offer a registration with the PAAS. We agree with this principle, as it suffices to have one strong authentication in place if the PAAS do not create a separate account or registration. It is common ground that account servicing PSPs need to provide strong authentication (cf. ECB 7th progress report, page 35). Thus, banks need to introduce strong authentication independent of the use of PAAS. This duty should be, as all stakeholders agree that, when using strong authentication, the perceived security issues with PAAS are largely resolved (cf. ECB Outcome Paper on the SEPA Council stakeholder meeting of March 25, 2013).

7.1 KC	**Authentication and agreement**	PMS usually do not have their own authentication for account holders using PMS. They do not need it, as they do not usually register users (see above). It should be made clear that 7.1 KC does not apply in that case. This could be achieved by repeating footnote 21 to define “where applicable”: *“Such as if the PAAS requires the customer to log in separately based on the registration with the PAAS.”* For ad-hoc use, the authentication of the user towards his bank can be relied upon. When authenticating toward his bank to confirm the transaction, he also automatically authenticates towards the service provider which initiates that same transaction. Furthermore, it should be made clear that PAAS without registration that do not fall under recommendation 7, do not have to seek agreement with the account-holding PSPs, as discussed in 7.1 KC second sentence. As set out before, the authentication of the account servicing PSP is in place and has to be used in any case, since otherwise the account holder would not be able to confirm his order to his bank. There is no alternative and an additional agreement would not change any security parameter. A duty to agree would effectively be a duty to have a contract with the respective bank before any PAAS could be offered. Thereby, banks would regain control over their competitors’ access to market by denying contracts. Past practice has shown that banks would not grant that access.

		Accordingly, a duty to contract would (just as the imposition of the four-corner model used for credit cards) exclude bank-independent PAAS from the market. This is why the Commission in the on-going legislative process pledged not to repeat mistakes of the past or as Vice President Almunia put it: *"(…) we need to avoid importing the issues that afflict the cards market into the new payment instruments.“* (SPEECH/11/889 of 14.11.2011) To sum up, multibank software services should not be under an obligation to install a separate authentication where they do not have accounts, user enrolment or registration. This would create an unnecessary and disproportionate burden (see guiding principle (ii), above). And they should not be forced to agree with banks in order to o be allowed forwarding user's orders to the bank account. Otherwise, market entry and competition would become impossible (see guiding principle (iii), above).

7.2 KC	**Strong authentic-cation**	As set out before, it should be made clear that this only applies where he PAAS has a prior registration. PAAS cannot influence whether the account servicing PSP has strong customer authentication for his account. The account servicing PSP has the sole responsibility for strong customer authentication for the payment account. In addition, the ruling of 7.2 is not really clear, especially the reference to white lists. Our proposal for 7.2 KC therefore would be: *"If a PAAS requires a separate authentication (based on a separate registration with the PAAS obtaining access to or amending sensitive payment data requires strong customer authentication for the registration with the PAAS . Where a PAAS offers purely consultative Services, with no display of sensitive payment data, the PAAS may adapt its authentication requirements on the basis of its risk assessment."*

8	**Enrolment**	To clarify that recommendation does not introduce a general duty to enroll customers, footnote 21 should be added to define "where applicable": *"Such as if the PAAS requires the customer enroll for the provision of*

		the respective services, e.g. if the customer has to log in separately based on a registration with the PAAS.”

10	**Monitoring**	The recommendations under KC 10.1 to 10.5 are generally sensible and to a large extent already best practice. Again there is no reason why these requirements should only apply to TPs and not to GAs. Accordingly they should be mandatory for all PIS. It should be noted that the range of possible checks is also limited by the applicable data protection laws of the Member States. For example the monitoring measures recommended under KC 10.2 would need to be designed against the background of the applicable provisions of data protection law in order to be entirely legal without consent of the merchant.

11	**Data Protection**	The requirements laid down under recommendation 11 should be mandatory for all PAAS, provided by TPs and GAs alike as well as covering bank-owned services and local stored applications (see guiding principle (i), above).

11.1 KC	**Merchant customer interface**	The requirement to secure data should be fulfilled by all actors involved in the transaction. The merchant, however, is not part of the transaction. As set out in 4.9 KC, he should not be involved. Accordingly, there is no customer interface of the merchant linked to the payment transaction. In particular, if 4.9 KC was implemented, the “consumer interface” of the merchant would not treat sensitive data that could be misappropriated or manipulated.

11.2 KC	**Merchant customer interface**	End-to-end encryption should apply for all services, i.e. TPs and GAs and also to any other multibank software services (see guiding principle (i), above). The potential risks are always the same.

11.3 KC	**Role of Merchants**	We support the position, that the e-merchant should have only the following information: Name of account holder, account number, bank, amount, reference, time, status of transaction (information he will also find on his banking slip), but no additional personal information from the bank account. The requirement that e-merchants may not receive “any sensitive

		payment data" could be too far reaching given the very wide definition of "sensitive payment data" in the glossary.

11.4 KC	**Proportio-nality**	The proportionality principle is a key principle that applies under the applicable data protection legislation. Under these rules, the customer agrees to the respective data checks that are necessary to provide the mandated service. However the details on how consent of the consumer is given and in which way, is already regulated in the data protection rules. We believe that there is no reason to impose stricter rules than required by data protection authorities, and notably no rules that conflict with data protection rules. Further, the recommendations has no mandate to do so. Therefore, the obligations should not go beyond the applicable legislation. Considering that to data protection laws may differ to some extent between Member States, given the remaining national competence in this field, 11.4 KC should simply refer to these national rules. The formula could be: *"The purpose of payment account access should be clearly determined and communicated between the TP and the customer prior to any attempt to access the payment account and the TP's involvement should be limited to the extent necessary to achieve this purpose ("proportionality principle") and to the extent permitted under data protection rules, without prejudice to the application of data protection rules."*

11.5 KC	**Storing data**	Given that the term "sensitive payment data" has been defined very broadly it should be noted, however, that it can be necessary to store basic data, e.g., the account number. As discussed before, SOFORT stores name, account number and bank of the originator as well as amount, date, reference, receiver and transaction ID with regard to a transaction. This information would normally be contained in the bank statement. SOFORT is under a legal obligation to document these data. The same data is also contained in the confirmation sent to the merchant (see remarks on 11.3 KC, above). In this respect, according the proportionality principle, PMS should not be hindered to store and use these data for the sole purpose of providing his service, as they are indispensable to provide the particular service. Moreover, these data occur in the bank statement in any case.

		Aggregation services will not be able to adhere to the above recommendation as such services necessarily require the storage of sensitive payment date, potentially all account data. SOFORT does not provide aggregation services. On that basis the above rules should be amended as follows: *"PAAS should not store sensitive payment data after the payment account access session of the account owner, unless this was necessary to provide the service mandated by the account holder ("proportionality principle"). To the extent that [PAAS] store data, they should ensure that the data are appropriately protected against theft and unauthorised access or modification."*

11.6 **KC**	**Using data**	It should be made clear that this includes the use of data necessary to provide the service, including all security features and measures against fraud. Notably, measures to prevent fraud by customers must remain possible. Again, data protection law provides a valid reference. Fraud protection measures normally are not "actively requested" by the customer (who may be a fraudster), but need to be applied by the service provider in its own and the merchants' interest as well as the general interest. In addition the term "actively requested" is not in line with existing laws. How to get the consent of the consumer should be up to the data protection rules. 11.6 KC could be amended as follows: *"TPs should not use personal account information for other purposes (e.g. for data mining, advertising, credit rating or data re-selling) than providing and enabling the service requested by the account owner, which may include fraud prevention mechanisms. This applies without prejudice to data protection legislation."*

11.1 **BP**	**Training**	Indeed e-merchants must handle sensitive payment data appropriately. This assumption contradicts, however, KC 11.3 according to which e-merchants should generally not be provided with "any sensitive payment data". Whereas SOFORT agrees that the amount of sensitive payment data provided to e-merchants must be limited to the absolute minimum, a general prohibition to provide them with any sensitive payment data is excessive if the term is defined as broadly as in the glossary of these recommendations. As set

		out above, the definition of “sensitive data” should either be less extensive – or the proportionality principle needs to be implemented instead of a per se prohibitions to use “sensitive” data.

11.1 **BP**	**Using data**	It should be noted that, in case the bank system does not distinguish between accounts, this rule should not lead the inability to provide services. Further, “expressly indicated” seems to be a very strong wording and should be replaced by “chosen” to avoid discussion on what form of approval would be required. Hence the wording would be: *“It is desirable that, to the extent technically possible, TPs only access data from the payment account chosen by the account owner for the payment account access session, and not the account owner's other accounts, such as savings or securities accounts or other payment accounts.”*

12	**Education**	Here again it appears that important duties should only apply to “TPs”. Instead they should apply to all multibank software services that allow access to the account over the internet (see guiding principle (i), above). For example, there is no reason that GAs should not adhere to such a common sense duty.

12.4 **KC**	**Discriminatory standards**	Under KC 12.4, the discriminatory treatment of “TPs” in contrast to GAs becomes very plain. There is no objective reason why the suggested requirements should always apply to TPs and to GAs only “where relevant”. It remains unclear in which cases the application of these standards would not be relevant for GAs. It must be recalled that GAs provide the same services as TPs and are exposed to identical risks.

12.5 **KC**	**Discriminatory standards**	The separation of payment-related processes from the online shop should be a mandatory security requirement for all multibank software services. Why should banks / GAs or local software applications not be subject to these rules?

12.7 **KC**	**Messages**	Such a requirement should not be interpreted in such a narrow meaning that the account servicing PSP would be enabled to technically interfere with the functioning of the TPs service. This would open up a backdoor to continue obstruction of bank-independent services under the cover of general security measures. For example, a

		strict duty to push any message of the bank, despite the fact that the message could be read at a later stage when the customer comes to his online account or that could be sent via e-mail, may offer a platform for bad-faith obstruction. In addition, the same obligation should apply to GAs.

12.8 KC	**Information**	KC 12.8 needs clarification. It should be recalled that multibank software services are subject to general requirements of data protection law. To this end SOFORT for example provides an extensive data protection notice which is accessible at every step of a transaction triggered by a PMS and which has been confirmed by the competent data protection authority. KC 12.8 should, however, not be interpreted in a way that additional, explicit confirmations must be actively declared by the customer which would effectively amount to a duty to "warn" customers of the use of the product and thus exceeds existing data protection law requirements. At any rate, requirements should apply to all multibank software services on a non-discriminatory basis to avoid distorting competition. 12.8 KC could be: *"PAAS should inform customers, at each payment account access session and in clear and simple language and according to the applicable data protection rules, that they will access specific sensitive data elements for the purpose of providing the service."*

12.9 KC	**Consent**	Generally, the same applies as noted under KC 12.8. meaning such additional requirements must not exceed existing data protection law requirements, should be limited to what is necessary to guarantee appropriate security standards and, importantly, should apply to TRs and GAs in the same way. In what from the consent for data use has to be given and which information has to be provided, is stipulated in data protection laws. The recommendations come up with the new term "expressly agree" and "clearly list each data element" that do not exist under data protection law, which will create room for interpretation and uncertainty.

		Further, it should be noted that PMS often do not have a framework contract, and the above rules should not impose a duty to conclude one. Information on what the software does provided before and during the transaction should be sufficient. 12.9 KC could be: *"The TP should provide information according to the data protection laws on any use by the TP of sensitive payment data. The information needs to be available before accessing the account as well as during the procedure and should list the data elements concerned according to the applicable data protection laws."*

13	**Limits**	If customers were supposed to set their own limits, this would indirectly require to introduce individual accounts, changing the business model and providing for immense complexity. We cannot see that such a high burden could be justified. In addition, if the aim was to prevent damages in case of misappropriation or abuse of authentication details, the limit should be imposed on the online account directly, where the limit protects for any direct and indirect access to the account. Therefore, the only effective way to prevent "high value fraud" is to set limits in the online banking account directly. This is already possible, therefore recommendation 13 would be a redundant overregulation and would not bring additional security.

13.1 KC & 13.1 BP	**Limits**	It should be recalled that every bank client (user) is generally free to define limits with regard to the use of his online bank account. Such limits cannot be circumvented by a TP if used by the client (or an unauthorised third party).

13.3 BP	**Personalisation**	Generally, the same reasoning as to 13.1 applies. So far such additional functions have not been part of PMS but provided by banks. As payment account access services are very secure they do not pose an additional threat to their users when compared to other online payment methods. Such security measures should therefore be installed at the online banking level where they can apply to all online payment methods the respective client uses and automatically apply to all PAAS used for this account..

14.1 KC	**Status of payment**	SOFORT rejects an additional requirement for TPs to provide a near real-time facility to check the status of the payment initiation to their clients. Such a requirement is (i) technically not feasible and misinterprets the specific role of a TP's service. It is (ii) also not necessary to guarantee the safety of the transaction. The services provided by TPs merely act as a messenger between the buyer and the seller. It is the role of the TP to inform its clients whether or not sufficient funds for a specific transaction were available the moment when the initiation was triggered and that the payment message was correctly transmitted to the respective Payment Account Service Provider. The TP has no access to the information whether or not the payment initiation was subsequently correctly executed by the Payment Account Service Provider. Accordingly, the TP cannot provide such information to its clients. Also such an additional facility to check would not significantly enhance, if at all, the security level of payments initiated by a TP. It should be recalled that the user (bank client) is free to access its online banking system and check the status of his account, particularly whether or not a specific payment was executed. Therefore, this recommendation would be disproportionate, leading to overregulation. It remains unclear what would be the added value of such a second level near real-time facility to check the Status of the payment initiation. This may have a reason within the internet recommendations, but not for PAAS.

14.1 BP	**Status of payment**	SOFORT agrees that it would be possible and could enhance the level of transparency to include the TP's band name and make the remittance information as comprehensive as necessary. While this would improve the practical use of the information by the client, not more data than necessary to achieve this goal should be included and potentially exposed. But it should be made clear that banks must not be allowed to abuse this additional information for discrimination and obstruction, as has been the case in the past.

GLOSSARY

As described above, the recommendations should apply to all PIS and AIS (together PAAS), regardless of their affiliation to banks or their place of storage. The following definitions should apply:

Payment Initiation Services *“the provision of software and related services to payment account holders, designed to enable payment account holders to access their payment accounts via the internet and initiate payments from their payment account, irrespective of the device or location where the service or software is being located (e.g. on a web-server or on a consumer end-device).”*

Account information Services *“Aggregation/visualisation services that collect information on different accounts held by an account owner with one or more account servicing payment service providers (PSPs) and that accesses the payment accounts via the internet, irrespective of the device or location where the service or software is being located (e.g. on a web-server or on a consumer end-device).”*

The term “TP” should be abandoned altogether, simply referring to PAAS, PIS or AIS – in order to ensure equal treatment. On that basis, also the term “GA” could be abandoned, as they would fall under “PIS”.

Finally, the term “sensitive data” should be limited to avoid overregulation:

Sensitive payment data Data which could be used to carry out fraud, but not the name of the consumer, his bank account number and his bank as well as other information available to the payee (merchant) on his banking slip.
These include data enabling a payment order to be initiated. data used for authentication, data used for ordering payment instruments or authentication tools to be sent to customers, as well as data, parameters and Software which, if modified, may affect the legitimate party's ability to verify payment transactions, authorise e-mandates or control the account, such as "black" and "white" lists. customer-defined limits, etc.