Note

PAYMENTS COUNCIL

12 April 2013

DL 020 3217 8423
Rhiannon.Butterfield@paymentscouncil.org.uk

To European Central Bank

From Rhiannon Butterfield

ECB CONSULTATION ON DRAFT RECOMMENDATIONS FOR 'PAYMENT ACCOUNT ACCESS SERVICES' - PAYMENTS COUNCIL (GB) RESPONSE

1 ABOUT PAYMENTS COUNCIL

The Payments Council is the body with responsibility for ensuring that payment services work for all those that use them in the UK. We work with payment service providers in the payments industry as well as other stakeholders to drive innovation in payments and implement change so that individuals and businesses have access to payments for their current and future needs.

We have three main objectives:

- To have a strategic vision for payments and lead the future development of co-operative payment services in the UK;
- To ensure payment systems are open, accountable and transparent, and
- To ensure the operational efficiency, effectiveness and integrity of payment services in the UK.

2 PAYMENTS COUNCIL (GB) RESPONSE - OVERVIEW OF KEY POINTS

Payments Council welcomes the opportunity to respond to the ECB's consultation on its draft recommendations for Payment Account Access Services (PAAS). The security of payments and the protection of customer data are of paramount importance, as is the integrity of the payment systems.

In general our response builds on the following key themes:

1. **Regulation of payment account access services**: Payments Council strongly supports the view that payment account access services (PAAS) should be regulated (e.g. via the Payment

Services Directive). Doing so will enhance competition and will allow the implementation of adequate consumer protection and security measures.

2. **Definition of the legal relationships:** Bringing payment account access services under regulation will also allow the legislators (if they wish to do so) to establish the certain rights and responsibilities of the parties in the payment chain. The legal relationship between the parties involved will vary by service, however, clarity as to by and to whom the services are provided is vital to ensure effective regulation. For example, it may be appropriate to allow services provided to corporates to opt out of consumer protection measures around transparency (but not, for example, security). Consequently we believe it would be preferable that these security recommendations only be finalised once the regulatory underpinning/legal framework for payment account access services has been established. Furthermore, there may be merit in revisiting the recommendations at a later stage to analyse whether they need to evolve to take into account further market developments as this is still a maturing sector. Finally, from a practical perspective, we believe that rather than having a separate (but ultimately very similar set of recommendations for PAAS services), it may be simpler in the long-term to include PAAS within the security of internet payment recommendations, with any PAAS-specific requirements clearly identified in a separate section.

3. **The security requirements for PAAS should not be considered in isolation** but as part of the broader discussions taking place around payment account access services (e.g. as part of the PSD Review process and in the EC/ECB Stakeholder meetings on internet payments). In particular, we believe that the following aspects are all inter-related and cannot be defined in isolation: (i) the legal relationship and service requirements between all parties in the payment chain; (ii) the rights, responsibilities and liabilities of PAAS as regulated entities; (iii) the security requirements that PAAS must comply with; (iv) and the definition of what elements should remain in the competitive space and/or where standardisation may be necessary.

4. **The recommendations should be thoroughly assessed against other legislative instruments** (such as the General Data Protection Regulation, the draft 4th Anti-Money Laundering Directive, the Regulation on e-Identification and Trust Services for Electronic Transactions, the proposed Directive on Network and Information Security (linked to the European Commission's Cyber Security Strategy), the Consumer Rights Directive, etc.) to ensure that their requirements do not conflict or that loopholes are formed, which might risk creating uncertainty and/or an uneven playing field. In particular, we note that a large amount of work has been done by a number of bodies in the area of **data protection and privacy**. The recommendations make a

number of references to relevant 'data protection legislation' but it is not clear the extent to which these recommendations have been analysed in detail against how this body of legislation already applies in this field. For example, 'sensitive payment data' as defined in the recommendations seems to include both payment transaction data and user authentication data, but may not include 'sensitive personal data'.

5. **Customer communication:** Further consideration needs to be given to the issue of communication to customers about the protection of their personal security credentials. Currently, Article 56 of the PSD (in conjunction with the terms and conditions of the account servicing PSP) is clear that customers should "take all reasonable steps to keep the personalised security features safe" and a great deal of effort has been expended in anti-fraud messaging to make this clear to customers. Thus there is potentially an inconsistency with regard to the use of some payment account access services that needs to be addressed. Once a legal framework around these services has been defined perhaps it may be useful for the Forum to organise a meeting between stakeholders so that a simple, consistent message for consumers can be agreed.

Using the template supplied by the ECB we have listed our detailed comments in section three below.

3 PAYMENTS COUNCIL COMMENTS ON THE DRAFT RECOMMENDATIONS FOR PAYMENT ACCOUNT ACCESS SERVICES

Originator: Payments Council (GB)

	Issue	Comment	Reasoning
1.	General comment	Suggestion	It is positive that the ECB is seeking to create a level-playing field by ensuring that all parties in the payment chain have to meet minimum security requirements. However, the topic of payment account access services is complex and there is a potentially wide impact for consumers and payment service providers (PSPs) alike, as well as implications for e-merchants. A number of issues around these services remain to be clarified, of which the security requirements are just one part. In order to properly address all of these issues we believe that a legal and regulatory framework around payment account access services needs to be defined. **Payments Council therefore strongly agrees that payment account access services should be regulated under the amended Payment Services Directive**. Once the legal framework is in place other issues, such as the form of the legal relationships between PAAS and AS PSPs, the types of services that need to exist between parties in the payment chain, definition of the areas that may benefit from standardisation or from being left open to competition, etc., can be explored in more detail and in context (we understand that some of these topics are already being addressed in the EC/ECB Stakeholder Meetings on Internet Payments). In addition, we support the inclusion of these services under the scope of the PSD because it will eliminate

			the lack of clarity around oversight that is bound to arise. The recommendations currently state that "*the legal basis for implementation of the recommendations is the existing oversight and supervisory competence of the relevant authorities*". Yet it is not clear how this interim measure would work in practice and further explanation would be welcome. There is a concern that this current approach could inadvertently, but most likely, lead to the creation of an uneven playing field as a result of varying security obligations in different jurisdictions. We believe that until the amendments to the PSD are published (and ultimately incorporated into national law) the legal basis for these services will be unclear, which is neither helpful for consumers nor other parties in the payment chain. For example, in the UK we would not expect the Financial Conduct Authority (FCA) to have jurisdiction over services provided by non PSPs/PIs, which are currently outside the scope of the UK Payment Services Regulations. We conclude that it would be logical for these PAAS recommendations to be finalised only once there is more clarity on the legal framework around these services (i.e. via the Payment Services Directive (PSD)). Then a more constructive debate on these services, their legal relationship with the AS PSP, and thus their rights and responsibilities with regard to data/consumer protection, can take place.
2.	General comment	Query	It is not clear the extent to which the PAAS recommendations (and indeed the security of internet payment (SIP) recommendations) have been analysed against other current regulatory proposals, such as the General Data Protection Regulation, the draft 4th Anti-Money Laundering Directive, the Regulation on e-Identification and Trust Services for Electronic Transactions, the proposed Directive on Network and Information Security, or the Consumer Rights Directive, etc. We see it as critical that these recommendations are not viewed in isolation but are assessed to ensure they can assist, or at least sit alongside each other and other relevant legislation, and do not open up loopholes, risking uncertainty

			and/or the creation of an uneven playing field. For example, the recommendations touch on issues of data protection and the uses of sensitive data. It would be useful for a thorough legal assessment to be carried out to ensure compliance with European and national data protection legislation, as well as other data protection initiatives (e.g. the PCI Data Security Standard), and to ensure that the definitions of key terms, such as 'sensitive payment data', are aligned with other legislative instruments. In addition, it is our understanding that a risk assessment of the various different methods of third party provider (TPP) access was undertaken by the ECB at the time the PAAS recommendations were being drawn up. If so, it would be helpful if these were shared to aid understanding of the recommendations.
3.	Scope	Clarification	It would be helpful to know whether these recommendations are intended to cover e/m-Wallets (where they have the same account access or payment initiation functionality) as well as third party providers. For example, an e-Wallet provider may guide the customer to an account with another PSP in the same way as some payment account access services do. Also, does the ECB intend that 'third parties' (as referenced in the recommendations) are only 'payment account information services'/'payment initiation services' and not more general third party service providers (or technical service providers)? Further clarity on this in the scope section of the recommendations would be appreciated.
4.	REC 1	Clarification	We would welcome an explanation/clarification as to the relationships (governance and otherwise) that the ECB envisages between the various entities – especially governance authorities (GAs) and TPPs. For example, will GAs have any role to vet TPPs, as we believe that it would be inefficient and impractical for

			PSPs to have to vet every TPP? The recommendations do not make clear what GA membership/accreditation is intended to convey. This raises a further question as to whether there may be merit in considering if GAs also need to be brought within the scope of regulation (e.g. the PSD) in order to ensure a level playing-field.
5.	1.2 BP	Clarification	Further clarity is required around what this best practice actually means. It refers to PSPs and TPPs '*defining minimum technical and security criteria for PAAS which are objectively necessary to reduce the potential risk associated with those services*'. If the PAAS services are part of a GA, will these criteria be defined multilaterally as part of the GA's 'formal security policy', or bilaterally between particular TPPs and PSPs? Are these criteria that would be in addition to these recommendations? We think it is important to avoid the setting of proprietary standards, even if these are communicated to 'interested parties'. Care needs to be taken to ensure that there is no perception of the use of multilateral standards to exclude some parties. Finally, it is not clear how the minimum technical and security standards developed between the TPPs and PSPs would be enforced. Customers and PSPs need assurance that minimum standards are being met to manage their own risks.
6.	2.1 KC	Query	We are supportive of the intention to require GAs and TPPs to consider potential risks to AS PSPs in their risk assessments. However, it is not clear how this would be achieved in practice without a formal relationship in place between the AS PSP and the TPP. For example, the KC suggests that the GAs and

			TPPs need to '*consider the risks associated with the chosen technology platforms, application architecture, programming techniques and routines… on the side of the AS PSP*'. It is difficult to see how the TPP would be able to measure the impact of their chosen IT technology on the IT infrastructure of the AS PSP unless this information is shared by the account servicing PSP. In general we note that a more formal relationship (such as a contract or protocol) between TPPs and AS PSPs is mentioned in or implied by some of the key considerations and best practices although there is currently no clear set of legal rights and obligations defined between the parties. Yet we note that in the security of internet payment (SIP) recommendations there is a repeated requirement on PSPs to ensure the integrity of security methods via contractual arrangements (see e.g. 3.4, 4.7, 4.8, 5.1 BP, 11.3). In addition, the definition of 'Account Servicing PSP' in the document glossary states that any outsourced functions should be under contract. We therefore conclude that a similarly formal relationship between AS PSPs and PAAS providers is both logical and crucial in order to properly define the rights and responsibilities of all parties in the payment chain, and indeed appears to be a prerequisite of many of these recommendations.
7.	3.2 KC	Query	The KC states that GAs and TPPs need to notify the competent authorities in the event of a major incident. However, the legal basis for doing this under the '*existing oversight and supervisory competence of the relevant authorities*' is unclear. For example in the UK, we would not expect the FCA to have jurisdiction over services provided by non PSPs/PIs which are currently outside the scope of the UK Payment Services Regulations. There is therefore no guarantee that incidents would be reported in a coherent and consistent way. This KC could be more easily achieved once the legal framework around

			these services (including GAs? See note 4 above) has been defined by bringing them under the scope of the PSD.
8.	3.1 BP	Amendment	Given the links with 3.3 KC, we think that the suggested requirements for TPPs, GAs and PSPs to inform each other of major security incidents should be a 'Key Consideration' rather than a 'Best Practice'. We note that 3.3 KC, 5.4 KC and 10.5 KC are all connected with how GAs, TPPs and AS PSPs respond to and deal with major incidents. As these are 'KCs' we think that it makes sense for 3.1 BP (which is about the notification that these major incidents have occurred) to be a KC as well. Such notification/liaison on major incidents will need to recognise the security risks inherent in information sharing and be guided by the purpose – dealing with the incident, preventing it from re-occurring, and/or learning best practice. It should be mandatory for all parties to coordinate in responding to security incidents, and logically such coordination responsibilities could be defined as part of the relationship in place between AS PSPs and PAAS providers.
9.	4.1 KC	Clarification	We think that this is a positive recommendation as it is important that any service that accesses payment accounts does not in any way undermine the security of the account, which is of paramount importance for privacy and data protection, as well as customer confidence. However, we believe that the KC could be further improved if the wording is updated from "*appropriate security and control measures*" to *"strong security and control measures"* (the 'comply or explain' principle would allow some flexibility for lower risk payment types). We also suggest that these measures must be properly supervised.

			We note that for the PAAS provider's risk assessment to be thorough and to ensure that the IT security of the account servicing PSP is not undermined, the AS PSP and the PAAS provider would probably need to engage with one another on a more formal basis.
10.	4.9 KC	Clarification/ Amendment	It should be clarified that not only should TPPs not authorise e-merchants to store sensitive payment data, but they must also seek to ensure that it does not happen. Furthermore, we suggest that GAs should also be covered by this KC as this will help to ensure that data loss/misuse is kept to a minimum. However, it is worth noting that if the merchants' websites are not secure then there will always be a risk of data loss. If sensitive data is misused or lost this will present a major risk to customers and the payment system.
11.	5.5 KC	Clarification	We request further clarification from the Forum on the intention/meaning behind the requirement for 'proper bilateral authentication' between TPPs and PSPs. We would encourage the use of existing communication/authentication methods as far as possible.
12.	5.6 KC	Query	We support this KC and believe it is vital for ensuring the integrity of accounts and for ensuring that any problems that the customer may encounter can be traced and the proper liability identified. However, it is not clear from the wording of the KC how this would be achieved in practice without being too complex and costly and we would appreciate further clarity around this (or perhaps further detailed discussion in a broader forum, such as the EC/ECB stakeholder meetings on internet payments).

			Putting cost and complexity aside, we also believe that in order for this recommendation to work in practice PAAS providers and AS PSPs would need a formal and on-going relationship in place in order to define the access criteria that will allow the AS PSPS to "*differentiate between payment account access by TPs and access by account owners without TP involvement*".
13.	5.1 BP	Clarification/ Amendment	We believe that, while perhaps being technically possible, a requirement for AS PSPs to provide customers with "*specific security credentials*" for use with PAAS will lead to confusion for the customer and may lead to payment errors. In addition, creating alternative credentials for customers to use when making payments through PAAS may require a major rebuild of the online banking services of AS PSPs, which we believe would be disproportionately costly and complex. Rather, we believe that it should be down to individual PSPs to define what is necessary to allow them "*to identify whether the account owner is making use of a payment account access service*" (based on their risk profiling and the relationship in place with the PAAS provider). This will ultimately lead to better security/protection for the customer as solutions can be tailored to specific risk profiles and can also take account of current market advances in, for example, biometric/natural authentication.
14.	6.1 KC	Query/ Clarification	It is not clear from this recommendation how the PAAS provider will know whether the customer has undergone the appropriate due diligence unless the information is supplied by the AS PSP. Further clarification of the wording would be helpful to ensure that procedures are adequate and well understood by all parties to avoid duplicating them at both the TPP and the PSP. Furthermore, it is important that clarity on the fraud and anti-money laundering responsibilities of PAAS is defined as part of the legal framework around these services. It is not clear from this recommendation

			whether the ECB believes that PAAS providers should be subject to know-your-customer (KYC) obligations. If so, it may be that they are able to rely on the checks undertaken by the AS PSP (although only if an appropriate relationship is in place between the two). Ultimately, it is vital that the use of PAAS does not disrupt PSPs' fraud prevention and anti-money laundering efforts.
15.	REC 6	Amendment	This KC requires that TPPs/GAs obtain confirmation of the customer's willingness to make use of payment account access services. We strongly believe that this consent (which should be affirmative and specific) also needs to be communicated to the AS PSP and ask that the wording is updated to reflect this. In addition, it would be helpful for the AS PSP to know that the necessary authority and transaction instructions are held by the TPP (both of these requirements could be built in to the legal relationship between the two parties). The PSP needs to have assurance that the mandate is properly implemented and that the service is being properly operated; it also needs to understand its liability in case of unauthorised transactions and those cases where its customer may have a claim against the TPP.
16.	REC 7	Amendment	We agree that strong customer authentication is required as both customers and TPPs require assurance that authentication is strong. We suggest that it might also be useful to add a section stating that GAs should set minimum standards.
17.	10.1	Query/ Clarification	This KC imposes a requirement on the TPP to "*identify suspicious transactions*". This may be complicated in practice given that the TPP may not have any transaction/behavioural history for the user, i.e. if the TPP is authorised to transact only once, it would not have access to the customer's payment history and could not therefore make a judgement about whether a transaction is suspicious. How does the ECB envisage this working in practice?

			In connection with this, further information/clarification would be welcome regarding a scenario where the AS PSP conducts analysis on a transaction that was initiated by a TP and then rejects it due to fraud concerns. We also believe that any fraud detection processes should be structured so there is no risk of 'tipping-off' when a transaction is turned down.
18.	10.2	Clarification	It is not clear what e-merchant activities the TPPs should be monitoring and we would welcome clarity on this point. Would it be in line with what is expected of merchant acquirers for card transactions?
19.	10.5 KC	Amendment	We believe that the duty to co-operate to deal with fraud or a dispute needs to be stronger and clearer and we ask that the language of this KC is updated to reflect this. At the same time, however, we also reiterate our earlier point that such co-operation to deal with fraud or a dispute needs to recognise the security risks inherent in information sharing and be guided by the purpose – dealing with the incident, preventing it from re-occurring, and/or learning best practice. We believe that for this to work in practice the duty to co-operate should be built into the formal relationship that needs to exist between all relevant parties in the payment chain.
20.	11.2 BP	Amendment	This best practice is positive in that it seeks to ensure appropriate consumer protection. In order to better accommodate payment account information services it may be better to say that TPPs should only access data from the "payment account**(s)**" specifically identified by the confirmation given by the account owner. It is crucial that the customer actively designates which payment account the TPP has access to but in the case of account information services (which 'provide information on several accounts held by a person with one or several PSPs') it would surely be necessary for the customer to have the option to

			designate access to more than one account. Nonetheless, it is critical that the choice regarding which accounts are accessed ultimately remains with the customer.
21.	12.3 KC	Amendment	We believe that the requirement that TPPs make assistance available to customers must be stronger and we think that the wording of this KC should be updated to reflect this. For example, consideration should be given to stipulating a single point of contact for customers to use in case of disputes. Without such an approach consumers may find themselves being passed from one party to the other (TPP, PSP, GA, e-merchant), possibly with no-one taking responsibility.
22.	12.4 KC	Query/ Suggestion	We believe that effective customer disclosures will be vital and we support efforts to ensure that customers can make informed decisions about the services they are making use of. However, we also note that it is potentially confusing for TPPs to educate customers on the need to protect their security credentials, yet at the same time the customer is making use of services that may require them to divulge their online banking credentials to a third party. Currently, Article 56 of the PSD (in conjunction with the terms and conditions of the AS PSP) is clear that customers "take all reasonable steps to keep the personalised security features safe". The inconsistency with regard to them giving these details to a third party therefore needs to be addressed. Once the legal framework around PAAS services has been defined perhaps it would be helpful for the Forum to organise a stakeholder meeting so that a simple, consistent message for consumers can be agreed.
23.	12.6 KC	Query	We believe that the overall aim of this KC – to improve transparency around liabilities – is positive. However, we note that this recommendation makes assumptions about the liability regimes of TPPs, despite the fact that wider stakeholder discussions concerning gaps in the current regime concerning the liabilities of the various parties in the PAAS payment chain are yet to take place, and will need to do so as

			part of the broader discussions on the legal relationship between all parties in the payment chain. For example, if these services are brought under the scope of the PSD then TPPs should be required to apply the same level of liability as PSPs as a minimum (i.e. the amount of the unauthorised transaction plus costs and charges). Liability regimes for TPPs and their customers should be harmonised as far as possible with the PSD to minimise customer confusion and to ensure a level playing-field. It is essential that customers understand the liability regime they are entering into when making payments via any kind of service, and how this may differ from other payment methods.
24.	12.9 KC	Possible amendment	We believe that the requirement for customers to give permission to TPPs to use data needs very careful consideration. Even if agreed, disclosure needs to be the minimum required to operate the services. It also needs to be ensured that any suggestions around the use of sensitive data are fully compliant with the General Data Protection Regulation. Customers are at risk if they disclose sensitive data. It needs to be clear that they understand the risks of doing so and that those TPPs can handle it safely. Perhaps it would be better if other methods were developed so no such disclosure is made.
25.	13.1 KC	Query	It is unclear how the limits applied by TPPs will work in conjunction with the limits of the AS PSPs. We presume it is intended that once the legal framework has been established, which will help to enable some form of formal relationship/protocol between TPPs and AS PSPs, PAAS providers will be in a better position to ensure that the limits they set for their service fall within the overall limits on the underlying bank account.

26.	REC 14	Amendment	In order to create a level-playing field and to ensure consistency for customers, we believe that the requirements on TPPs to provide information to customers about payments should be modelled on the current PSD requirements, especially if PAAS are brought under the scope of the PSD. PSD requirements are tried and tested; customers are increasingly familiar with what they can expect from the PSD formats and may be confused by different information provision. We would prefer the wording of the recommendation to reflect this (albeit that these TPPs are not yet regulated under the PSD).