11 April 2013

International Banking
135 Bishopsgate
London EC2M 3UR

Telephone: +44(0)20 7678 0670
Facsimile: +44(0)20 7085 4003

European Central Bank
Secretariat Division
Kaiserstrasse 29
D-60311 Frankfurt am Main
Germany
ecb.secretariat@ecb.europa.eu

Dear Sir / Madam,

Re: Recommendations for "Payment Account Access" Services (PAAS)

The Royal Bank of Scotland plc (RBS) welcomes the opportunity to comment on the SecuRePay proposals for PAAS. Being an operator of a major retail and business banking network, RBS is keen to support innovation, but in ways which ensure our customers' are not exposed to excessive risks.

As requested we have made our detailed comments in the attached pro forma. We would, however, like to emphasise some high level points of principle.

In general the proposals are helpful in defining the security environment in particular, but there is a need to establish more clearly the legal and contractual framework within which they will work.

Legal framework – RBS firmly believes that PAAS providers, especially those offering Payment Initiation Services, should be regulated and supervised under the PSD. This will help ensure proper protection of the integrity of the payment system and define consumer rights.

Contractual framework - there should be a contractual framework, covering liabilities based on dual consent by account holding customer and Account Servicing PSP with respect to the Third Party. The relationship between Third Party service provider and the Account Servicing PSP is mentioned in some of the Key Considerations and Best Practices, but these combined do not result in a clear set of rights and obligations between the parties.

The contractual framework should have sufficient freedom for stakeholders to compete freely. However, a set of liabilities / obligations should also be agreed as a standard, in order to avoid a difference in interpretation across member states.

Governance Authority – the role of the GA should be more clearly defined in matters such as standards setting and dispute resolution. It should act as a scheme body.

If the PSD review does not bring PAAS into regulation, a strong GA will be especially important as an alternative source of authority to ensure adherence to security standards. This is likely to require the contractual framework described above.

Commercial - there should be clarity on the business model. As additional costs will undoubtedly be incurred by all the stakeholders involved, the business model should explain how reasonable costs of the various parties can be recovered.

I hope these comments are of assistance. If it would be helpful RBS would be very happy to discuss the PAAS proposals with you.

Yours sincerely

Kevin Brown
Managing Director- Global Head of Transaction Services Product
RBS, International Banking

Comments on the Recommendations on "Payment Account Access" Services
RBS input

Originator	Issue	Comment	Reasoning
The Royal Bank of Scotland plc, UK	Payment Account Access Services (PAAS), P2	Clarification: The role of the Governance Authority (GA) should be clarified. Is it a scheme or scheme body? Its nature and role will need to be defined; it will need to have powers to enforce standards such as those described in this document. In order to promote competition, the scheme should be open to any operator which meets objective criteria which protect payments integrity.	The Governance Authority has a key role to play in making PAAS work. Without it there does not appear to be a body to enforce standards and adjudicate on disputes. In its absence all the various parties would need to make bilateral agreements. The absence of either will bring a high level of risk to customers and the payment system.
	Objective, P2	Amendment: The Security objective is fully supported. In addition there should be a clear legal and contractual framework to support PAAS.	Without a clear legal (see Implementation below) and contractual basis to enforce the security requirements we believe that achieving the security objective will be extremely difficult. Contracts could be bi-lateral or part of the underpinning of a scheme.
	Scope, P3	Clarification: Do these guidelines cover eWallets as well as Third Party Service providers?	The eWallet provider may guide the customer to an account with another PSP.
	Guiding Principles, P3/4 a	Amendment: PAAS providers should state clearly in their agreements with GAs, PSPs and customers whether they are providing Payment Initiation Services or Account Information Services.	This will make clear which service the Third Party (TP) is providing and guide which customer accounts they can access and for what purpose. This will reduce the risk of misunderstanding of the purpose of the TP and ensure proper control.
	Guiding Principles, P3/4 b	Amendment: The principles and standards in this document should be required of PAAS providers.	The document frequently states that its standards "should" be adhered to. To safeguard the payments system, these "must" be adhered to.
	Implementation, P4	Clarification: The suggestion in the paper that Account Access Services are brought within the scope of the	Until changes to the PSD are incorporated into EU/domestic laws, the legal basis for these services is unclear**.** For

		PSD is helpful. In the meantime it is suggested that "Currently, the legal basis for implementation of the recommendations is the existing oversight and supervisory competence of the relevant authorities". It is not clear how this interim measure would work in practice and further explanation would be welcome.	example in the UK, we would not expect the Financial Conduct Authority automatically to have jurisdiction over services provided by non-PSPs which are currently outside the scope of PSRs.
	Implementation, P4	Amendment: There is a need for a clear business model consistent with principles of a competitive market.	All parties will incur costs in providing this service. There should be mechanisms for recovery of reasonable costs, including cost of capital, by all affected parties.
	Rec. 1 a.	Clarification: Will the GA have a role in approving TPs such that PSPs themselves need not vet the TP and its procedures?	It would be inefficient for PSPs to have to vet every TP.
	Rec. 1 b.	Amendment: The security policy should be based on international security standards.	These are widely recognised and may be easier to apply than a bespoke standard.
	1.2 BP a.	Clarification: It is not clear whether the minimum technical and security standards will be defined multilaterally as part of the GA's duties or bilaterally between particular TPs and PSPs.	The parties need to know where they stand. If multi-lateral standards are used, care needs to be taken to ensure that there is no perception of use of these multilateral standards to exclude some parties.
	1.2 BP b.	Clarification: It is not clear how the minimum technical and security standards will be enforced.	Customers and PSPs need assurance that minimum standards are being met to manage their own risks.
	Rec. 3	Amendment: Consideration should be given to a requirement that where customer security is breached this should be disclosed to the customer.	Such a requirement will be especially required if the PSP is not involved in the breach (and may be unaware).
	3.3 KC a.	Amendment: A procedure is required that describes how the TP and PSP will co-operate in the event of a security breach.	In the event of a breach, clearly defined processes and responsibilities will ensure that it is rectified as quickly as possible.
	3.3 KC b.	Amendment: In the event of a major breach of security the PSP should have the right to suspend the service pending resolution of the breach.	PSPs will need to protect the payment system, their customers and themselves from an ongoing breach of security. There is otherwise a risk of unquantified losses occurring.
	3.1 BP	Amendment: Change "could" to "must".	It is essential that information on major security breaches is

			shared to enable all parties to take action to prevent it spreading or recurring and to address resulting customer needs.
	4.1 KC	Amendment: "Security and control measures" will need to be strong and minimum requirements made clear to all parties. These must be properly supervised.	There is a risk to payment system integrity and so all parties must be very clear about their duties.
	4.7 KC	Amendment: There must be external audits of security measures, not only internal audits.	Although internal audits are valuable these themselves must be verified externally from time to time to ensure they are independent and objective.
	4.8 KC	Amendment: There is an option for TPs to outsource functions related to the security of payment account access services. Out-source providers and their systems will need to be subject to rigorous audit and testing.	Account Service PSPs and their customers will require assurance that no party involved in PAAS is introducing additional risk into the payment system.
	4.9 KC	Amendment: Not only should TPs not authorise e-merchants to store sensitive payment data, they must ensure it does not happen.	Were sensitive data to be misused or lost this will present a major risk to customers and the payment system.
	5.1 KC	Amendment: The suggestion that PSPs should offer customers different log-on credentials for use with TPs from their usual log-on will enhance security and the audit trail, but is likely to be costly and cumbersome to implement. Customers may forget or confuse log-on credentials.	This approach is likely to require a major rebuild of online banking services. Alternatively the TP should provide a flag to identify the transactions in which it is involved. However, if no more cost effective alternative can be found, a mechanism will be required for the PSP to recover these and other reasonable costs from the TP .
	5.5 KC	Clarification: Requirement for bilateral authentication between TP and PSP requires further clarification.	This is a new requirement on PSPs. As far as possible existing communication/authentication methods should be used.
	5.6 KC	Amendment: There is a requirement for account servicing PSPs to differentiate between payment account access by TPs on the one hand and account owners without TP involvement on the other. While logical this may be complex and costly.	This is a new requirement for PSPs and could have a significant impact on PSP systems. Though helpful in terms of managing risk and providing a clear audit trail of transaction, PSPs will incur costs. As at 5.1 KC above, a mechanism will be required for the PSP to recover these and other reasonable costs from the TP.

	Rec.6 a.	Clarification: There is a requirement for TPs/GAs to obtain customer's consent. This information would need to be shared with the PSP. How would the account holding institution ensure that the same authority and transaction instructions are enforced by the TP?	The PSP needs to have assurance that the mandate is properly implemented and then the service is being properly operated. It needs to understand its liability in case of unauthorised transactions and those cases where its customer may have a claim against the TP.
	Rec.6 b.	Clarification: Customer consent is essential, but the legal environment needs to be clarified.	In general PSPs do not currently allow their customers to do anything which might result in disclosure of their log-on credentials to third parties. This is seen to be in line with PSD Article 56 obligations on the service user.
	Rec.6 c.	Amendment: At no point should sensitive information such as PINs and passwords be entered into a TP system.	The basis of account access security requires that log-in credentials are known only to the customer. Disclosure could compromise security and confuse liability.
	6.1 KC	Clarification: Due diligence procedures for new customers need better definition. We assume that KYC and AML are included. Will the PSP be able to assume all such checks have been done to the standards required of the PSP itself?	It is necessary to ensure that procedures are adequate and well understood by all parties and avoid duplicating them at both the TP and the PSP.
	6.2 KC a.	Clarification: There is a reference to liability as between TP and customer. We assume that there is no new liability for PSPs.	All parties must be clear as to their risk and liability. PSPs not involved in a transaction should not be liable.
	6.2 KC b.	Clarification: If the TP is insolvent how are any outstanding claims resolved?	Customers, merchants and PSPs will need assurance that outstanding claims will be repaid or, at the least, clarity about where they stand in an insolvency.
	Rec. 7	Amendment: We agree Strong Customer authentication is required. The GA should set minimum standards and the actual processes should be independently audited.	Customers and AS providers and TPs require assurance that authentication is strong.
	7.2 KC	Clarification: The circumstances in which a TP can amend sensitive payment data need to be clarified.	In general we would not expect TPs to have a role in amending payment data as this is a matter for the customer. However, if there are exceptional circumstances where the TPs might do so legitimately these should be explained.

	8.2 KC	Amendment: Customer enrolment for strong authentication should be mandatory.	Customers should benefit from the most secure environment possible.
	Rec. 9	Amendment: TPs must always apply a limit to the number of log-on attempts by the customer.	This is standard good practice to reduce the incidence of fraud.
	10.1 KC	Clarification: There is a requirement on the TP to "monitor abnormal behaviour patterns of the customer". It is not clear how this would work in practice.	If the TP is authorised to transact only once, it would not have access to the customer's payment history and could not undertake this work. If the PSP does the analysis, what would happen if the TP initiates a transaction which is then rejected by the PSP due to fraud concerns? Processes should be structured so there is no risk of 'tipping-off' when a transaction is turned down.
	10.5 KC	Amendment: The duty to co-operate to deal with fraud or a dispute needs to be stronger and clearer (we assume that any risk of contravening AML, tipping off requirements etc can be dealt with).	There is a risk that some parties may take advantage of a weak requirement to avoid co-operation.
	Rec. 12	Clarification: Customer communications will be vital. It will be a very considerable piece of work.	It is essential that customers understand the liability regime they are entering into when using a TP and how this may differ from other payment methods.
	12.3 KC	Amendment: The requirement that TPs make available assistance to customers for questions, complaints, etc needs to be stronger. In particular consideration should be given to 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 (TP, PSP, GA, e-merchant), possibly with no-one taking responsibility.
	12.6 KC	Amendment: It is suggested that TPs can put a cap on their liability to customers. They should be required to apply the same level of liability as PSPs as a minimum (the amount of the unauthorised transaction plus costs and charges).	Liability regimes for TPs and their customers should be harmonised as far as possible with PSD to minimise customer confusion and ensure a level playing field.
	12.9 KC	Amendment: The requirement for customers to give permission to TPs to use data needs very careful consideration. Even if agreed, disclosure needs to be	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 TPs can handle it safely. It would be better if

		the minimum required to operate the services.	other methods were developed so no such disclosure were made.
	Rec. 14	Amendment: Requirements on TPs to provide information to customers about payments should be modelled on PSD requirements.	PSD requirements are tried and tested. Customers are increasingly familiar with the PSD formats and may be confused by different information provision. There should be a level playing field.

11 April 2013

In case of query please refer to David Malley, +44 (0) 20 7678 3544 David.Malley@NatWest.com