ECB-PUBLIC

Comments received on the recommendations on the security of internet payments

Contact details: Prof. Dr. Jürgen Bott,
jbott@jbott.de
+49 (0) 6021 5827199, +49 (0) 171 26 78 409

Originator: Prof. Dr. Jürgen Bott
University of Applied Sciences Kaiserslautern, Germany
ISO code of the country of the originator **DE**

Comments on the recommendations for the "payment account access" services

Originator	Issue	Comment	Reasoning
Jürgen Bott, DE	Scope	The exclusions are not always comprehensible, especially the exclusion of: -traditional online payments (via internet) - mobile payments other than browser-based payment (general separation of browser-based payments) - clearing and settlement of payment transaction (unclear definition: is this exclusion restricted to the exchange of clearing data between banks?, please refer also to comments to Recommendation 14 and the General Part)	Running payment accounts (executed by Payment Account Service Providers) and transmitting payment instructions between Account Owners and Payment Account Service Providers (transmitted by Payment Initiation Service Providers or by Payment Service Providers) are two types of services, which should be distinguished. Sometimes both services are offered and operated by the same legal entity. Ownership structures or contractual arrangements between the entity which provides the account services and the entity which provides the transportation services of the payment instruction should be irrelevant for the minimum security standards (minimum expectations) applied to payment initiation services. Also Governance Authorities (GA) and Third Parties (TP) should be treated equally. All organisations providing account access services (regardless whether they are owned by credit institutions or by non-banks) should – with respect to account access services – fulfil the same minimum security standards and should be controlled (supervision / oversight) equally. In its assignment to initiate a payment transaction all types of licensed service providers (under supervision/ oversight) should be able to operate on a level playing field. Payment initiation services are always and exclusively executed on behalf of the Account Owner. Obligations of Payment Service Providers and Payment Initiation Service providers should be the same (with respect to online access to payments accounts) and minimum security standards should be defined regardless of contraction arrangements (if any at all) or ownership structure between Payment Account Service Providers and the Payment Service Providers or Payment Initiation Service Providers.

Jürgen Bott, DE	Implementation	Minimum expectations for account access services have to be the same for any type of service providers. Ownership structure or contractual arrangements between Payment Account Service Providers and the organisation which provides the account access services have to be irrelevant for setting minimum expectations or the level of supervisory or oversight regulations.	Once the providers of payment account access services (Account Information Service Providers and Payment Initiation Service Providers) are regulated under the revised Payment Service Directive, payment account access services will be limited to licensed institutions. The members of the Forum expressed their commitment to support the implementation of the recommendations in their respective jurisdictions and to integrate them in existing supervisory/oversight frameworks. PSD has the intention to foster competition in the payment business by opening the market to new types of service providers. If the recommendations are intended to provide interim guidelines until revised PSD will be enforced, recommendations have to be clearly worded, not to arouse suspicion to hamper competition during interims period. Recommendations for "Payment Account Access" Services should support the intention of the PSD.
Jürgen Bott, DE	Recommendation 2: Risk assessment, Especially 2.1 KC	It seems to be disproportionate to oblige Third Parties and Governance Authorities to carry out and document **detailed** risk assessments for payment account access services, **including potential risks** to the account servicing PSP from the performance of payment account access services.	All providers of account access services are supposed to be regulated under the revised Payment Service Directive and common securities standards for these services will be integrated in supervisory/oversight frameworks. To what extent will Third Parties or Governance Authorities be in the position to execute an assessment of potential risks to the account servicing PSP which will be more meaningful than the risk assessment continuously performed by the supervisory / oversight authorities? 2.1 – 2.4 KC seems to be the orientation for proper supervisory / oversight standards, which have to be commonly applied to any provider of payment account access services.
Jürgen Bott, DE	Recommendation 4: Risk control and mitigation especially 4.5 KC in relation to Recommendation 5: Traceability	4.5 KC requests Third Parties to ensure "data minimisation" (policy of gathering the least amount of personal information necessary to perform a given function) might be a) in contradiction to Recommendation 5 asking Third Parties to ensure that all	Traceability of all transactions (in the requested manner) and customer due diligence procedures (including identity documents) before granting access to payment account access services require that Third Parties have to store sensitive data extensively. To avoid contradiction between "data minimisation" request and appropriate demand for traceability and due diligence

	and 6.1 KC (customer due diligence procedure with identity documents) and in some respect also Recommendation 10: Monitoring and Recommendation 14: Customer access to information on the status of payment initiation.	transactions, as well as the payment account access process flow, are appropriately traced and b) in contradiction to 6.1. KC which requests Third Parties to ensure that the customers have undergone the customer due diligence procedures, and have provided adequate identity documents and related information **before** being granted access to payment account services.	(including ex-post evidence that Third Parties obligations have been fulfilled correctly) it seems to be necessary to distinguish more precisely between the obligations of the Payment Account Service Providers and the organisations which provide exclusively access to payment accounts (i.e. account information services and payment initiation services). Payment Account Service Providers are responsible that anti-money laundering regulations are fulfilled. Only Account Owners who already went through a careful due diligence process are allowed to initiate payment transactions between payment accounts (i.e. between different Payment Account Service Providers or between accounts run be one Payment Account Service Provider). Third Parties providing account information service have lasting contractual relationships with their customers. However, the pure information service about account statements does not trigger transactions with anti-money laundering issues. Third Parties providing payment initiation services have in general two types of contractual arrangements. With E-Merchants they have lasting contractual relations. Within this contractual arrangement it is feasible to perform some kind of due diligence. (However, we have to keep in mind that E-Merchants would have to go through careful due-diligence twice, first time with the Payment Account Service Provider (when opening the payment account) and the second time with the Payment Initiation Service Provider (when asking for special initiation service provided by a Third Party). If the Payment Account Service Provider performs its anti-money laundering obligations correctly, it is questionable what quality gains the second due diligence process of a Third Party will bring.) It is a quite different story with respect to the due diligence requirements Third Parties should perform with consumers (e.g. shoppers at E-merchants' internet platform) who request Third Parties' services only on an "ad hoc" basis. It is neither efficient to ask consumers who request Third Parties' payment initiation services only on an "ad hoc" basis to go through a second thorough due-diligence procedure (after careful due diligence already performed by the Payment

			Account Service Provider of the consumer), nor is it expected that this second due diligence will bring significant additional anti-money laundering intelligence. Such a request would hamper Third Parties' ability to compete with Payment Account Service Providers, which are offering their own payment initiation service. Furthermore, there is no reasoning given, why 4.5 KC should be limited to Third Parties and does not include Governance Authorities.
Jürgen Bott, DE	Recommendation 5: Traceability especially 5.6 KC	Account Servicing PSP should be able to differentiate between payment account access by Third Parties and access by account owners without Third Party involvement.	Third Parties act exclusively on behalf of the Account Owner. As long as legitimatized security measures (which are not slanted towards hampering competition) agreed between Account Owner and Payment Account Service Provider are followed, it is up to the Account Owner to decide which software to use to instruct his/her Payment Account Service Provider. If identification of the Third Party Payment Initiation Service Provider or Account Information Service Provider (e.g. via IP-Address) will be mandatory, it has to be ensured that identification method will never be misused for discriminating Third Parties.
Jürgen Bott, DE	Recommendation 6: Initial customer identification and information	The entire section seems to be very much oriented on the recommendations for the security of internet payments.	Customer due diligence; please see comments given to recommendation 4): A more differentiated approach is indispensable.
Jürgen Bott, DE	Recommendation 7: Strong customer authentication especially 7.1 KC	7.1 KC could bear the risk of inconsistency, under the assumption, that Third Parties provide their payment initiation services exclusively on behalf of Account Owners,and they have to follow strictly the legitimated binding contractual arrangements between the Account Owner and her/his Payment Account Service Provider. We have to keep in mind: The strong customer authentication method to access payment accounts is agreed between the Account Owner and the Payment Account Service Provider. The Third Party (providing payment initiation services) may act only	Payment Account Service Providers are responsible to protect their Accounts Owners' funds. The Payment Account Service Provider agrees with its Account Owners (at least) on one of the "strong customer authentication procedure" (as described on page 9 of the Recommendations for "payment account access"). If Account Owner decides to use the payment initiation service of a Third Party, the Account Owner has to apply the strong authentication method agreed with her/his Payment Account Service Provider. The Third Party (providing the payment initiation service on behalf of the Account Owner) has to follow strictly the advice received by the Account Owner. The Third Party only transmits Account Owner's instructions (including the data required by the strong authentication procedure agreed

		(exclusively) as a messenger, which has to follow strictly to the Account Owner's advice. In order to access Account Owner's account the Third Party will have to meet the requirements of the authentication method agreed between Account Owner and Payment Account Service Provider.	between the Account Owner and the Payment Account Service Provider). If the message transmitted by the Third Party (from the Account Owner to the Payment Account Service Provider) is not of the quality that Payment Account Service Provider can undoubtedly authenticate the Account Owner, payment may not be initiated (i.e. Payment Account Service Provider has to refuse receipt of the instruction). There is no need for an additional agreement between the Third Party (providing the payment initiation service) and the Payment Account Service Provider. The only applicable strong customer authentication method is already agreed between the Account Owner and the Payment Account Service Provider. The agreed authentication method has to be applied regardless of the way the payment instruction is transported between the Account Owner and the Payment Account Service Provider.
Jürgen Bott, DE	Recommendation 14: Customer access to information on the status of payment initiation	Third Party - which only initiates payment – can't be held responsible for internal procedures of Payment Account Service Providers.	Payment Initiation Service Provides act only as a messenger assigned by the Account Owner to transmit a payment instruction to her/his Payment Account Service Provider. The messenger (Third Party) can only inform the Account Owner whether her/his instruction was successfully transmitted to her/his Payment Account Service Provider. (Under the request, that access data are not stored by the Third Party:) Third Party can't inform the Account Owner about the correct execution of the instruction within the operations of the Payment Account Service Provider. On instruction of the Account Owner, Payment Initiation Service Providers can also inform payee that payer has instructed his Payment Account Service provider to execute a transaction (i.e. to pay a bill). Third Party can't inform payee whether (all involved) Payment Account Service Providers have executed instruction (in real time). In general the Payment Initiation Service Provider has no information whether and how the Payment Account Service Provider executes a properly received payment instruction. In some cases several Payment

			Account Service Providers are involved in executing the payment process between the payer and the payee (e.g. via correspondent banking networks). Usually Third Party Payment Initiation Service Providers are not involved in the correspondent banking networks. Account Owners can use e.g. online banking facilities to set limits and to check account status and to view proper execution of instructions sent to the Payment Account Service Provider. Third Party Service (account information services) can support the Account Owner in processing "online banking information" and/or present the account information in a more user-friendly way and/or combine account information from several Payment Account Service Providers. In general the Third Parties' account information services are limited by the data, which are – in accordance to the contractual arrangements between the Payment Account Service Provider and the Account Owner – disclosed by the Payment Account Service Provider. Please check also whether Recommendation 14 is in accordance with "Scope and Address" (exclusion of "clearing and settlement of payment transactions"; please see above issue on scope).
Jürgen Bott, DE	General Part and Glossary of Terms Third-party service providers (TP)	Minimum expectations outlined in the recommendations for payment account access services should be applied to all service providers, regardless whether they are in a contractual arrangement (including outsourcing agreements) with the Payment Account Service Provider or not.	The report claims to provide recommendations to improve the security of payment account access services, to foster the establishment of a harmonised EU/EEA-wide minimum level of security and to focus on the whole processing chain of electronic retail payment services (excluding cheques and cash), irrespective of the payment channel. Under this guideline it is to expect, that the minimum standards apply to all providers of payment account access services.