SecuRe Pay Forum

“Recommendations for the security of internet payments”

Comments of German Banking Industry Committee (GBIC)

General Comments

The aim to achieve finality and non-repudiation of remote payments is generally supported. However, the Forum should take into consideration that PSPs with their service offering for remote payments compete with other providers which seem to be exempted from the proposed recommendation. Such exemptions do not only create disparities in competition, but they could also cause a heterogeneous customer experience when carrying out remote transactions. Already from a competition point of view, it is necessary that all kind of remote payments, regardless whether they have been initiated via cards, CT, SD, via a transfer of money between e-money accounts, via a credit transfer where a third party accesses the customer's account or via corporate cards or even anonymous cards, are subject to the same recommendations without any exemption.

Some clarification would be appreciated concerning the scope as it is not clear whether online banking offering SCT and SDD is affected. Online banking is not a scheme but an individual service offered by banks to their customers only. In addition, it is up to each individual bank to decide to offer online banking services or not.

Remote payments are offered by schemes which are competing with each other. Therefore, the proposed recommendations should rather address such schemes than individual PSPs, who are anyhow obliged to follow the rules of the schemes they are participating in. Finally, it is up to the various remote payment schemes to incorporate the proposed recommendations in their scheme rules and to require implementation by their participants.

The implementation of strong customer authentication is indeed an appropriate means to achieve non-repudiation of transactions. However, the proposed recommendations should not only clarify that the implementation of other authentication means than a strong customer authentication will not lead to a proof that the customer has authorised the transaction, but it should also clarify that in case of a strong customer authentication a clear proof of authorisation by the customer is given.

If strong customer authentication is implemented, which delivers finality and non-repudiation of transactions, the level of monitoring should be proportionate to the level of security required and strength of the customer authentication method used. If a transaction is clearly attributable to the customer and to the merchant any fraudulent transaction can have occurred only due to gross negligence of the customer or the merchant. PSPs should not be required to implement additional systems to detect and prevent potential gross negligent behaviour of their customers. This would go beyond what PSPs could provide and it could even dilute the responsibilities between customer and PSPs in terms of reasonable care. Whether PSPs are offering to their customers additional means allowing steering their risk individually with remote payments should be left to the individual product policy of the PSPs.

Recommendation 1 Governance

The addressee should rather be the schemes which are providing remote payments than individual PSPs.

Recommendation 2 Risk identification and assessment

The addressee should rather be the schemes which are providing remote payments than individual PSPs.

Recommendation 3 Monitoring and reporting

The addressee should rather be the schemes which are providing remote payments than individual PSPs.

Recommendation 4 Risk control and mitigation

The addressee should rather be the schemes which are providing remote payments than individual PSPs.

KC 4.2 seems to go too far into technical details because they could hamper quick responses to new security threats. It is expected to restrict the recommendations to technology-independent security aims rather than specific technical implementations. In addition it should be taken into account that a strong customer authentication provides a very good means to mitigate many of the risks addressed in KC 4.2, so that some of the additional security measures may prove not to be necessary. In line with Recommendation 2 it should be left to the individual risk assessment on scheme level to define the detailed security measures to be applied to achieve the ultimate aim of finality and non-repudiation.

Recommendation 5 Traceability

The addressee should rather be the schemes which are providing remote payments than individual PSPs.

Recommendation 6 Initial customer identification, information

KC 6.1 It must be assured that the identification procedures have to applied to all providers of internet payments, not only PSPs.

KC 6.2 There are too many detailed requirements, PSD Article 42 seems to be sufficient.

KC 6.3 It should be clarified that there is no requirement for PSPs to control the spending behaviour of customers generally. Whether PSPs are offering to their customers additional means allowing steering their risk individually with remote payments should be left to the individual product policy of the PSPs.

Furthermore it should be taken into account that the requirements of the PSD has already led to a huge increase of information provided by PSPs to customers, which has caused not only considerable costs, but also complaints from customers. The implementation of specific information duties for PSPs with regard to remote payments could increase the amount of information to be given to the customer and it could even be detrimental to the wide-spread acceptance of such remote payment systems.

Recommendation 7 Strong customer authentication

Recommendation 7 goes too far into technical details because they could hamper quick responses to new security threats. The recommendations should be restricted to technology-independent security aims rather than specific technical implementations. In addition it should be taken into account that a strong customer authentication could already mitigate many of the risks addressed in Recommendation 7, so that some of the additional security measures may prove not to be necessary. In line with Recommendation 2 it should be left to the individual risk assessment on scheme level to define the detailed security measures to be applied to achieve the ultimate aim of finality and non-repudiation. Accordingly also the liability shift as proposed in KC 7.6 might be dispensable and should not be required as a general rule anyway.

Furthermore it should be taken into account that 3D-Secure is not an example for strong authentication method but just a protocol which could enable strong authentication. In addition, CVx2 is not comparable to a strong authentication mechanism, as breaches are possible and known. Accordingly, it is proposed to delete any reference to a specific implementation (i.e. 3D-Secure and CVx2) and just to refer to the security aims to be achieved.

KC 7.1 The requirements regarding e-mandates should be reconsidered as e-mandates are used only for information and do not initiate final payments.

KC 7.2 It should be clarified that access to account balance information, balance history etc (eg log in to online banking) is out of scope.

Recommendation 8 Enrolment for and provision of strong authentication tools

Also Recommendation 8 - although agreeable in terms of it's aims - seems to go too far into technical details. It is expected to restrict the recommendations to technology-independent security aims rather than specific technical implementations. With regard to card payments it should be taken into account that PSPs may have already well-accepted procedures in place for providing customers with security credentials like cards and PINs which may not necessarily comply with the detailed provisions of Recommendation 8, but which have proven to be very effective.

Recommendation 9 Log-in attempts, session time-out, validity of authentication

Recommendation 9 is going too far into technical detail. The Recommendation shall be limited to security aims, which have to be considered in the security policy of any scheme providing remote payments and where appropriate measures have to be defined to achieve these aims.

Recommendation 10 Transaction monitoring and authorisation

The level of monitoring should be proportionate to the level of security required and strength of the customer authentication method used. For example, real time fraud detection and prevention systems are only indispensable in the case of real time authorisation, guarantee or settlement. It should also be clear that whilst the role of the issuer is key in detecting fraudulent activity, the acquirers can also help their customer base in the reduction of potential fraud.

It should be clarified that there is no requirement for PSPs to control the spending behaviour of customers. Whether PSPs are offering to their customers additional means of steering their risk with remote payments should be left to the individual product policy of the PSPs.

Recommendation 11 Protection of sensitive payment data

According to Recommendation 2 any scheme should be required to assess the risks associated with its remote payment scheme. This risk assessment should identify the risks and threats to the scheme and it should identify which data have to be considered as sensitive together with the measures to protect these data. As such Recommendation 11 is regarded as dispensable and it should not require the implementation of specific technical solutions regardless of the individual security assessment for the scheme affected.

Recommendation 12 Customer education and communication

Customer information takes already place today to a large extent and there is no need to require further customer information with regard to remote payments. It should be taken into account that the implementation of the PSD has already led to a huge increase of information to customers, which has caused not only considerable costs, but also complaints from customers. The implementation of specific information duties for PSPs with regard to remote payments could increase the amount of information to be given to the customer and it could even be detrimental to the wide-spread acceptance of such remote payment systems. In general: information only if the measures used for remote payment need to be explicitly explained.

Recommendation 13 Notifications, setting of limits

As explained above, the implementation of additional means for customers to control their spending behaviour should be left to the product policy of individual banks. The implementation of such measures is considered as something which goes beyond the security of payments, with the potential to create an additional safety feeling from the point of view of the customer.

Recommendation 14 Verification of payment execution by the customer

No comment

Comment to Annex

All of the recommendations seem already to be covered by the existing PSD and its implementation into national law. There is no need to change the PSD in this respect, especially with regard to the information to be delivered to customers or liability.