Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

Stellungnahme

Comments by Die Deutsche Kreditwirtschaft (German Banking Industry Committee)[1] on the proposal of the European Commission for a revised Payment Services Directive (PSD 2)

Kontakt:
Roland Flommer
Telefon: +49 30 20225- 5548
Telefax: +49 30 20225-5545
E-Mail: roland.flommer@dsgv.de

Dr. Kai Zahrte
Telefon: +49 30 20225- 5367
Telefax: +49 30 20225-5345
E-Mail: kai.zahrte@dsgv.de

Berlin, 19. Dezember 2013

Federführer:
Deutscher Sparkassen- und Giroverband e. V.
Charlottenstraße 47 | 10117 Berlin
Telefon: +49 30 20225-0
Telefax: +49 30 20225-250
www.die-deutsche-kreditwirtschaft.de

[1] Registration number of Die Deutsche Kreditwirtschaft in the European Union transparency register: 52646912360-95.

Contents

I. Introduction and overview

On 24 July 2013, the European Commission presented its "Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC" (COM(2013) 547/3). The Deutsche Kreditwirtschaft welcomes that the European Commission only sees a need to change certain points in the EU Payment Services Directive. The EU payment law only came into force in the EU member states in November 2009, and only those changes should be made that address a particular need for improvement. Otherwise, the payment law should remain unchanged so as to ensure legal certainty, to limit the adjustment burden for payment service providers and users to the absolute minimum and maintain the smooth functioning of the Single Euro Payment Area (SEPA).

From the viewpoint of the Deutsche Kreditwirtschaft, some of the changes to the EU Payment Services Directive proposed by the European Commission still need considerable improvement.

Particularly, there is significant need for action concerning the

- changes to the payer's unconditional right for a refund of a direct debit (Article 67 paragraph 1, see II.1.),
- civil-law regulations for third party payment service providers (Articles 58, 59 and 87, see II.2., and Article 65 paragraph 2, see III.1.a.), and also
- regulations on strong customer authentication (Article 87, see II.3.).

In addition, there is a need for improvement concerning the changes relating to information and execution obligations and also concerning the liability regime (see III).

II. Points with particular need for improvement

1. Article 67 paragraph 1 - the existence of the SEPA Core Direct Debit Scheme must be protected. Restricting the payer's unconditional right to a refund is not in the interest of payment service users and providers.

With Article 67 paragraph 1 last subparagraph, the European Commission would like to codify an unconditional right for a refund of a payer which is a consumer for a SEPA core direct debit (no-question-asked principle), as claimed by consumer protection associations on the one hand, and exclude the right to a refund under framework terms for a "no-refund scheme" as advocated by individual companies, if the payee has fulfilled his contractual obligations towards the payer, on the other hand. However, the proposed measure does justice to neither set of interests and actually jeopardises the existence of the SEPA Core Direct Debit Scheme:

a. There is nothing wrong with codifying an unconditional eight-week right for a refund for the consumer as the payer of a SEPA core direct debit, because so far the SEPA Core Direct Debit Scheme Rulebook has declared this "no-question-asked" principle as binding. The Article 62 of the current EU Payment Services Directive supplies a stable legal basis for such contractual

arrangements.

b. The restriction of the right for a refund envisaged in Article 67 paragraph 1 last subparagraph of the proposed directive is, however, inappropriate for those cases in which the retailer/service provider has yet to render performance:

- Merging the payment transaction and underlying transaction with respect to a right to a refund means that the unconditional eight-week right for a refund which a payer currently has in the SEPA Core Direct Debit Scheme would in effect be reduced to a few days and even removed in a number of cases. This approach significantly worsens the legal situation for the consumer and in no way reflects the payer's expectations when using a direct debit. The SEPA Core Direct Debit Scheme would lose a great deal of its attractiveness, which would also be to the detriment of the payee side.

- Nor could payment service providers in retail payments transactions (in Germany almost 9 billion direct debits per annum) implement the requirement of Article 67 paragraph 1 last subparagraph that they should review every individual direct debit refund request arising from an objection by the payer (in Germany currently some 130 million transactions) for possible non-performance and disputes in the underlying transaction. The direct debit scheme could no longer continue to be operated at its current low cost.

- A change to the refund rules in the SEPA Core Direct Debit Scheme would void all the obtained direct debit mandates to date, because these contain an unconditional eight-week refund right for the payer as a fundamental principle pursuant to the SEPA Core Direct Debit Rulebook. This would greatly disadvantage payees above all, because they would have to obtain new direct debit mandates from their payers in order to continue the direct debit payment arrangement with them. In Germany, this would affect an estimated volume of over 800 million mandates.

From this it follows that Article 67 paragraph 1 last subparagraph has to be amended such that it codifies an unconditional right to a refund for the payer of 8 weeks from the debit date without restrictions. In addition, to avoid any misunderstandings, it or a relevant recital in the directive should reaffirm the current principle of a separation of the payment transaction and underlying transaction, whereby the payer's refund claim against his payment service provider in the payment transaction has no implications for civil-law claims of the payee against the payer under the underlying transaction (e.g. payment of the purchase price for a good sold and supplied).
To take the need for framework terms for a "no-refund scheme" into consideration as assumed by the commission, the directive could give the contractual parties – payment service providers, payer and payee - the right to conclude such contractual agreements under certain preconditions.
However, it must be ensured that such an arrangements are part of a separate rulebook between payment service providers that is to be distinguished from the EPC rulebook for the SEPA core direct debit. Only a clear distinction between the procedures will protect the existence of the SEPA core direct debit and enable the consumer to continue to rely on an unconditional right for a refund under this scheme.

2. Article 58 – appropriate precautionary measures must be taken for the use of "third party payment service providers".

With Article 58, the EU commission is looking to promote competition in payment transactions by opening the bilateral technical customer-to-bank interface for "payment initiation services" pursuant to Article 4 number 32 and "account information services" pursuant to Article 4 number 33. To that end, "third party payment service providers" (see Article 4 number 11), should be able to initiate payments for the payer, for example via online banking, and be able to gain a full insight into his or her account information (inter alia balance, transaction turnovers). This means payers are to be allowed to disclose personalised security features (e.g. Online PIN and TAN) to third party payment service providers. The commission's proposals on this, in particular Article 58, are in need of considerable improvement in order to not only provide third party payment service providers with a business model, but also to sufficiently honour the interests of the account servicing payment service provider operating the technical customer-to-bank interface and also the interests of their customers. The objective must be to develop a harmonious overall concept that balances economic interests and protects the integrity of the technical infrastructure. In addition, due attention must be paid to property rights, consumer protection, data protection and banking confidentiality.

a. Payer's right to use third party services (Article 58 paragraph 1) – reinforcing control over the technical customer-bank interface

(1) Inclusion of the account servicing payment service provider

The technical customer-to-bank interface (e.g. online banking) is based on a bilateral contract between the customer and his bank and therefore belongs to both the bank and the customer. Just as the bank may not make this bilateral interface accessible to a third party, customers have no rights of their own to open the interface to third parties. This particularly applies if third party payment service providers gain their own economic advantages from using the interface – as can be observed in the market for example where the added value extracted from such access is sold as a separate service, e.g. to an online retailer. Therefore, expanding the use of the interface must also be dependent on the consent of the account servicing payment service provider (double consent approach).

(2) Protecting the integrity of the technical infrastructure

Uncontrolled opening of the technical customer-to-bank interface for third party services would greatly jeopardise the integrity of the account servicing payment service provider's technical infrastructure. Today, electronic customer access to payment service providers enjoys the customer's almost unlimited trust. Without the possibility to control access to the technical infrastructure, and thus to ensure reliability, availability and security of the systems, there would be a risk of a total loss of trust in electronic customer access to payment service providers with practically unforeseeable consequences for the payment service provider's customer relationships (online banking is nowadays an indispensable customer relationship tool) and for the economy as a whole.
Controlled opening of electronic customer access should be based on regulations in the form of security requirements for technical interfaces, but also on organisational requirements in the form of emergency plans, for example. Compliance with these regulations would have to be proved in a certification audit. Only certified third party services agreeing to meet the organisational requirements and to carry out the required technical changes within a reasonable period of time would be allowed to use the electronic customer access. Suitable technical measures enable authorised access to be distinguished from unauthorised access.

This normal market approach is demanded by supervisory bodies for acceptance networks in card-based payment transactions and has proven itself over the course of twenty years.

(3) Payer's activation instruction

Should, contrary to (1), the payer be given an unrestricted right to use third party services, then a precondition for opening the interface should be that the payer first issues an activation instruction - preceding the payment order – directly to his or her account servicing payment service provider in order to protect the security of the technical customer-to-bank interface and to protect payers as well. The account servicing payment service provider should only then open the interface for the third party payment service providers named by the payer. This ensures that the technical customer-to-bank interface is not open from the very beginning, but is accessible to certain third party services only and in so far as expressly wished by the customer. This is an important precaution against fraudulent attacks on the customer-to-bank interface. At the same time, it would create the technical preconditions that enable the payer to refuse certain third party services access to the customer-to-bank interface again at any time (see also (3)). A comparable control and protection mechanism for the payer already exists today in the direct debit scheme (see Article 5 paragraph 3 d) i) and iii) EU SEPA Regulation[2]), under which payers can open or block their accounts with respect to the collection of direct debits from certain payees.

(4) Payer's blocking options

In order to preserve the payer's and the bank's rights of control over the customer-to-bank interface, the following should be allowed for

- the payers' right to block their account to "third party payment service providers", and
- the account servicing payment service provider's right to block the interface, should the third party payment service provider lose its regulatory approval or to ward off acute threats to the technical customer-to-bank interface (e.g. hacker attacks).

b. Access by third party service providers to the payer's personalised security features (Art. 58 paragraph 2 a) – Protecting the need for confidentiality

(1) Third party payment service providers do not need access to the payer's personalised security features to render payment initiation services.

For security reasons and to protect banking confidentiality, third party payment service providers should not have any access to the payer's personalised security features (e.g. Online PIN/TAN). For this is tantamount to being given the "master key" to issue payment orders and to view all the payer's account information (e.g. the customer's complete financial status for the last 180 days). This gives third party payment service providers far too much control over the payer's account, despite it not being required:

- In the light of the availability of funds information from the account servicing payment service provider pursuant to Article 58 paragraph 3, payment initiation

[2] REGULATION (EU) No 260/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euros and amending Regulation (EC) No 924/2009

service providers need no access whatsoever to the customer's entire account information for rendering their services in online retailing. The availability of funds information in itself suffices for the payment initiation service provider to be able to inform the online retailer about the successfully triggered payment so that the retailer in turn can arrange for the delivery of goods.

Nor do third party payment service providers need any direct access to the payer's personalised security features for passing on the payer's payment order in favour of the online retailer to the account servicing payment service provider. There are technical processes in which payers - without the possibility of access by third party payment service providers - can send their personalised security features directly to the payment service provider, despite the payer's actual payment order being submitted to the account servicing payment service provider by a third party payment service provider. This means that only at the account servicing payment service provider stage is the incoming payment order combined with the personalised security features sent directly by the payer. For example, a so-called "Central Online Banking Site" (COB, see **Appendix 1**) could be set up so that the third party payment service provider can submit payment orders to the account servicing payment service provider whilst at the same time always ensuring that payers can enter their online customer PIN and TAN directly in the account servicing payment service provider's system (e.g. online banking site of the account servicing agent). The relevant market participants could define the specification for the COB interface. If necessary, the newly created European Retail Payments Board could monitor these standardisation activities. The assurance by the third party payment service provider to comply with the COB interface specification would have to be defined in Article 5 as a precondition for approval by the supervisory body.

(2) Restricting the use of personalised security features

Should, contrary to (1), third party payment service providers be permitted access to the payer's personalised security features (e.g. Online PIN and TAN), then avoiding misuse risks and safeguarding the payer's data protection rights require the following procedure: customers must first explicitly instruct the account servicing payment service provider to activate the account for the stipulated third-party service provider. Also in the event of such an activation, it must be laid down that third party payment service providers may use these personalised security features solely for transmissions to the account servicing payment service provider. They will also be prohibited, inter alia, from using these authentication means to evaluate the payer's entire account information for a creditworthiness check or to produce a behaviour profile and from disclosing account information to third parties. Thus the scrutinisation of the customer's complete financial status by third party payment service providers using automated and ultra-fast processes – as is being intensively done today by various third party payment service providers – would be prevented, as would a malware attack on an inactivated account that is concealed as a third-party service.

c. Authentication by third party payment service providers to account servicing payment service providers (Article 58 paragraph 3 b and Article 87 paragraphs 2 and 3)

Third party payment service providers have to authenticate themselves upon activation in the customer-to-bank interface to the account servicing payment service provider with separate

authentication means that permit unique identification of the third party payment service provider. This is a prerequisite for ensuring that the customer-to-bank interface is only accessible to those third party payment service providers with regulatory approval pursuant to the EU Payment Services Directive and whose payers who want to have access to the interface. The authentication methods should meet pertinent ISO standards and, following extension of Article 87 paragraph 3 of the proposed directive, the EBA could set binding minimum requirements.

d. Storage prohibition concerning payment data and personalised security features (Article 58 paragraph 2 c)

To ensure that customers remain sovereign over their account data and personalised security features, third party payment service providers may use these data solely to render the payment initiation services and must delete them once the transaction is completed. In addition, to avoid the creation of customer profiles (see above), third party payment service providers must not be permitted to read and evaluate the account information data made accessible by dint of the payer's personalised security features. Completely opaque scrutinisation of account information to evaluate payers' behaviour must be excluded so as to safeguard data protection.

e. Availability of funds information to third party payment service providers (Article 58 paragraph 3)

The obligation of the account servicing payment service provider to give availability of funds information to third party payment service providers is meant, above all, to secure the business model of online payment service providers already active in the market whereby the online retailer is given information about the payment transaction without procurement of a payment guarantee by the account servicing payment service provider, so that the retailer can initiate the delivery of goods or the rendering of services. Since third party payment service providers themselves generate an economic benefit with the "credit check" they call down, i.e. make a profit from reselling private information from the account servicing payment service provider's databases, the directive must include a possibility for the information providing payment service provider to charge the information beneficiary (= third party payment service provider) a reasonable fee. Otherwise, the directive would in effect lay down that the information from the bank is free whilst allowing third party payment service providers to sell that same information to retailers. Such an outcome is not compatible with the principles of a free market economy principles or with the protection of account servicing payment service providers' property rights. Moreover, it would also be unlawful interference in the copyrights of the database producer (here the account servicing payment service provider) protected by Article 7 of Directive 96/9/EC ("EC Database Protection Directive") – see also Section 87b German Copyright Act – because the account servicing payment service provider has made a considerable investment in setting up the database infrastructure necessary for the online banking. Under Section 87e German Copyright Act, access by a third party is possible only on the basis of a use agreement with the database producer.

3. Article 59 – preservation of the high level of security in card payment transactions

Our comments on third party payment service providers which use the online banking infrastructure of account servicing payment service providers also apply mutatis mutandis for third party card issuers and the infrastructure of the card payment systems.

a. Unclear regulation

It should firstly be noted that the scope of Article 59 is extremely vague. This is in part because the terms "third party payment instrument issuer", "payment card services" and "payment card" are not given a legal definition. Furthermore, the recitals give no indication as to which business model is being promoted.

b. No distortion of competition by so-called "free riders"

Regardless of the concrete form of the apparently not yet practised business model of third party card issuers, it is hard to fathom from a competition perspective why the providers of a technically incomplete – and hence possibly lower priced – product such as a payment card without the corresponding payment transaction infrastructure (so-called "free riders") should be supported.

c. No diluting of account servicing banks' security standards

In so far as account servicing payment service providers will be obliged in the future to permit account access with cards from third party issuers, it must at least be ensured that the issued cards meet the same security standards as the cards which account servicing payment service providers themselves issue. Banks in Germany issue cards that meet the highest available technical security standards. This they do because they continuously strive to keep misuse as low as possible so that the lowest possible risk costs are priced into their charges. Third party issuers do not have this motivation, but are interested in the most economical production of cards possible, because high security standards do not pay off for third party issuers.

4. Article 87 - ensuring the reasonableness of demands on authentication means

The payer's authentication means play a major role in the security of payment transactions. Hence it is only logical that - following in the steps of the European Banking Supervisors' SecuRePay Forum - Article 87 attaches particular banking regulatory importance to "strong customer authentication". Having said that, there is still considerable need for improvement here too:

a. Strong customer authentication (paragraph 1 sentence 1)

- The definition in Article 4 No. 22 is definitive for the specification in Article 87 paragraph 1 of a "strong customer authentication". This goes beyond the definition in the European Banking Supervisors' SecuRePay Forum recommendation on internet payments in that it defines additional requirements above and beyond the factors of possession, knowledge and existence. These conditions are hard to grasp from the wording and technically scarcely implementable. It should be sufficient to implement two factors - possession, knowledge or existence.

- The scope of Article 87 paragraph 1 is limited to "electronic payments" which the payer "initiates". However, the chosen wording does not allow the intended issues to be clearly perceived. What is probably meant is online banking transfers and card-based payments involving payment instruments (i.e. online banking PIN / TAN or debit card and PIN for example), whereas direct debits initiated by the payee are actually to be excluded. Such a distinction is appropriate, but should be made much clearer in the regulation.

- Under Article 87 paragraph 1 sentence 1, there must be "strong customer authentication", unless the EBA guidelines allow specific exemptions. Just like in the preceding chapters of the directive, a distinction based on relevance should be made in the directive itself. For example, simple customer authentication may suffice for payment transactions of small amounts (up to 30 euros per transaction). For these low-value payments in particular, there must be a sensible balance between cost and benefit.

- The regulatory regime is too focused on customer authentication and gives insufficient heed to other technical precautionary measures already in use. For example, one-factor authentication can indeed achieve comparable overall security, if highly developed background systems that help to identify and prevent fraudulent attacks on the customer account are also used for payments. Hence the regulatory approach must be made much more flexible as a whole so as to accommodate the wealth of technical solutions.

b. Secure customer authentication for third party services (paragraph 1 sentences 2 and 3)

- Every payment service provider, i.e. including third party payment service providers, should provide their own authentication methods. There is no apparent reason from the security or level playing field perspectives why third party payment service providers should be given beneficial treatment in that they can resort to methods provided by the payment service provider.

- In addition, it must be borne in mind that it is not even technically possible for an account servicing payment service provider to make certain authentication means available (e.g. in the case of a qualified electronic signature under the EU Signatures Directive and the German Signatures Act). Sentence 2 would otherwise mean that payment service providers would be prohibited from using qualified electronic signatures or the electronic proof of identity of the new personal ID card in Germany for customer authentication for example, because third party payment service providers would not necessarily be in a position to use them too. Such a requirement would be extremely dubious and untenable under the security policy aspect. Therefore, the provision in sentence 3 [sic] must be struck out.

- Should the approach nevertheless be maintained, it would have to be clarified as to how the third party payment service provider can remunerate the account servicing payment service provider for using its authentication methods. This should be left up to market forces and a contractual agreement.

c. Authentication of third party services towards the account servicing payment service provider (paragraph 2)

So that the payment service provider can fulfil its duties under Article 58 paragraph 2 b, it must be defined here not only that the third party payment service provider has to authenticate itself to the account servicing payment service provider, but also how this is to be done. Reliable authentication serves the security interests of all involved, third party payment service providers too, who would otherwise run the risk of their name being misused. The supervisory authority should ensure that this authentication is not weaker than that which the customer uses for authentication for payment service providers. Hence authentication of the third party payment service provider by its IP address would be totally unacceptable for security reasons.

d. EBA guidelines (paragraph 3)

The directive should express more clearly that the EBA guidelines on customer authentication methods must not lead to a single or only a handful of authentication methods being used. For the greater the reduction in permissible methods, the fewer targets there will be for illegal attacks and hence the greater the risk of a widespread effect of those criminal attacks. In other words: a plurality of suitable authentication methods protects against systemic risks.

Paragraph 3 should be amended to read that the EBA and ECB are also responsible for describing and developing authentication media with which third party payment service providers can authenticate themselves towards account servicing agents pursuant to paragraph 2.

III. Other points requiring improvement

1. Liability law – the scope of responsibility of payers, payment service providers and third-party service providers must be given due consideration in liability law (Articles 65, 66, 80).

a. Article 65 paragraph 2: no liability of the account servicing payment service provider for losses caused by third-party service providers

Article 65 paragraph 2 lays down that the account servicing payment service provider is to be held liable for unauthorised payment transactions even if the cause for the transaction lies with the payment service provider used by the payer. Such a burden of liability is completely unjustified, because under the approach of the Commission's proposal third party payment service providers are in no way in the account servicing payment service provider's camp but full-square in that of the payer. Furthermore, so far it has been exclusively the payer who selects and resorts to the third party service. The account servicing payment service provider has so far had no means whatsoever to exercise influence concerning the third party service. To nevertheless impose liability for the third party service on the account servicing payment service provider runs counter to each and every principle of liability in civil law and is unreasonable. Instead, there must be an independent provision for the payer to hold the third party payment service provider liable. Only such a direct recourse will ensure that the third party payment service provider remains answerable for its shortcomings towards its customers and hence bear liability for the same. Such a liability model is also an additional motivation for the third party payment service provider to use the most secure technical processes and systems possible. The account servicing payment service provider should not be liable to the payer under Article 65, if it can prove that it is not answerable for the cause for the unauthorised payment transaction.

Should the solution proposed above not be taken up, then the payment agent's recourse claim against the third party service provider envisaged in Article 65 paragraph 2 sentence 2 should be formulated as a ground for claims. Since the third party payment service providers is not in the payment agent's camp, the aforementioned disadvantages for the payment agent should be mitigated at least in part by increased liability and defining the burden of proof appropriately. For example, there should be strict liability on the part of the third-party service provider towards the payment agent, i.e. a causal fault by the third party payment service provider shall in itself be sufficient for liability. In addition, the burden of proof should not be on the payment agent, which should have a reimbursement claim unless the third party payment service provider can prove within the short period of time of one week that the unauthorised payment transaction did not arise from a fault on its part.

b. Article 66: no modification of currently valid liability rules and amounts so as to maintain the payers' motivation for careful handling of their payment media

In retail payments transactions, it is essential to strike a balance in liability issues so that payers have faith in the form of his perspective relatively risk-free system, whilst at the same time encouraging a minimum degree of diligence in handling their payment media through a reasonable involvement in the risk. This serves on the one hand to create acceptance for the payment method and on the other hand prevents losses from high misuse levels being socialised.

(1) Preserve the payer's EUR 150 liability risk when using payment media (paragraph 1 sentence 1)

- There is no call for reducing the payer's liability to EUR 150 [sic] in the event of unauthorised use of payment cards. In view of the payer's actual powers of disposal, this liability limit has always been relatively low, but was nevertheless sufficient to motivate payers to keeping their cards safe. The proposed reduction to EUR 50 however, falls below the psychologically important floor of a three-digit liability amount.

- Nor should it be overlooked that this liability relates only to the period from when the card is lost to when the card blocking notification is received by the payment service provider (see paragraph 2). It is not apparent why a cardholder who notices the loss of his card but fails to immediately report it and thus acts recklessly concerning a loss through unauthorised use should from now on be required to share liability only to such a trivial amount.

- All in all, it is to be feared that reducing the liability limit will considerably weaken the customer's motivation to submit a card blocking notification immediately after noticing the card's loss or misuse of his payment media. The losses arising for the payment service provider from delayed card blocking notifications are ultimately borne by all the customers because risk increases can impact the fee structures of payment service providers.

(2) Payments via a distance communication where no strong customer authentication is required (paragraph 1 sentence 3)

- Firstly, it should be noted that the liability of the payee and payment service provider is not clearly expressed here. But apparently joint and several liability is envisaged for the event that no strong customer authentication is required on the payee side.

- This liability rule errs in reducing the payer's liability in fraud scenarios. In principle, payment services law assumes the payer's liability for intention and gross negligence, whereby the burden of proof for this tends to be owed by the payment service provider. This in itself constitutes a major shift of the liability regime compared with normal civil-law principles. Why the payer's liability for intention and gross negligence is now to be excluded as well if strong customer authentication is not offered is not at all clear. It should be borne in mind that such a process requires regulatory approval, i.e. must be audited and admissible. If a payer who uses one of these permitted processes fails to take any care whatsoever or even knowingly and intentionally causes harm, that payer is not worthy of any protection at all. Nor can the particular aspects of the process lead to a different outcome, for a process that has been so designed is not conceivable or would never be approved by a supervisory body.

- Exempting payers from liability for intention and gross negligence as well would surely lead to a considerable increase in misuse figures. The resulting losses would be borne by all those involved in the process, for only in the rarest of cases will it be possible to prove the payer's mens rea required for fraud.

c. Article 80 paragraph 1 subparagraph 4: only liability for the delay loss for late execution of payments

The Payment Services Directive in the past lacked a clear provision that the payer's payment service provider had to compensate for the delay loss and not, for example, the payment amount in the event of late receipt of a payment by the payee's payment service provider. On the face of it, this problem seems to have been rectified by Article 80 paragraph 1 subparagraph 4. However, the wording is wide of the mark. Instead, delay loss compensation should be stipulated.

2. Fulfilling information duties - admissibility of modern forms of communication as an alternative to postage in the pre-contractual stage and following changes in payment service master agreements (Articles 44, 47)

The information duties introduced by the Payment Services Directive (PSD I) with effect from November 2009 has meant that after a current account has been opened or when general terms and conditions are changed, bank customers have to be sent e. g. up to 35 pages of contractual text, which by and large simply parrots the wording of the legislation. Changing the direct debit terms and conditions in the German banking sector in 2012 thus led to some 2,000 tons of paper being sent by post.

This in turn led to numerous bank customers complaining about the "waste of paper" and telling their banks not to submit any more paper-based GTC change proposals. By dint of the receipt requirement laid down in Article 44 payment service providers cannot comply with that request even if it is the express wish of their customers.

To promote the stated objective of the revised EU Payment Services Directive, namely to foster new internet-based processes, the requirement should be that pre-contractual information only has to be offered to customers (e.g. as an internet download). To accommodate the customer's interest in a manifested contract, it suffices that there first be a presentation of the content of or changes to the

contract in simple words and attention be drawn to the right to demand the complete text on paper free of charge before the contract is signed, and also at any time thereafter (see Article 46).

This ecologically and economically meaningful change would at the same time protect payment service users from information overload.

3. Regulatory requirement for better implementation of recovery in the event of incorrect transfers (Article 79 paragraph 1)

Article 79 correctly lays down (as the former Article 74 in the previous version) that a payment order can be executed in accordance with the unique identifier and comparison against the name of the payee is not required. This priority of the unique identifier remains necessary for fully automated processing of payment orders and for meeting the very short execution deadlines.

However, it should be noted that payers may encounter problems in getting their money back when transfers are misrouted due to an incorrect unique identifier. The arrangement now envisaged in Article 79 paragraph 3 to minimise the problem has proved to be incomplete. This requires the payer's payment service provider to make reasonable efforts to recover the funds involved in the payment transaction. In practice this leads to difficulties, because the payee's payment service provider has not so far has been expressly obliged to participate and can cite problems under banking confidentiality for disclosing the name and address of the unjustly enriched payee. This information is, however, indispensable for the payer's legal steps. Therefore, Article 79 paragraph 3 should be amended to read that the payee's payment service provider has a duty to cooperate. If the payee refuses to return the funds wrongly received by dint of the transfer, the payee's payment service provider must then disclose the name and address of that payee.

4. Re Article 3 litt. k and l: no new exceptions from the scope of the directive

Article 3 lit. l excludes certain services with a payment character rendered by telecommunications companies from the scope of the directive. The already existing range of exemptions has in effect been extended in that the offered services no longer have to be related to the end device used for the order. As a result, the exceptions are too vague. It should also be borne in mind relating to telecommunication services in particular that there are especially high risks of money laundering and dubious services (e.g. use of special phone numbers etc.). Therefore, the exemption for electronic communication networks / services should be struck out in its entirety. This is not inequitable, for micro-payments are already given special treatment, so that such services will continue to enjoy the same privileges as before. The same applies concerning the exception in Article 3 lit. k.