June 2012

AK Position Paper

Position on the Green Paper

Towards an integrated European market for card, internet and mobile payments

www.akeuropa.eu

About us

The Federal Chamber of Labour is by law representing the interests of about 3.2 million employees and consumers in Austria. It acts for the interests of its members in fields of social-, educational-, economical-, and consumer issues both on the national and on the EU-level in Brussels. Furthermore the Austrian Federal Chamber of Labour is a part of the Austrian social partnership.

The AK EUROPA office in Brussels was established in 1991 to bring forward the interests of all its members directly vis-à-vis the European Institutions.

Organisation and Tasks of the Austrian Federal Chamber of Labour

The Austrian Federal Chamber of Labour is the umbrella organisation of the nine regional Chambers of Labour in Austria, which have together the statutory mandate to represent the interests of their members.

The Chambers of Labour provide their members a broad range of services, including for instance advice on matters of labour law, consumer rights, social insurance and educational matters.

More than three quarters of the 2 million member-consultations carried out each year concern labour-, social insurance- and insolvency law. Furthermore the Austrian Federal Chamber of Labour makes use of its vested right to state its opinion in the legislation process of the European Union and in Austria in order to shape the interests of the employees and consumers towards the legislator.

All Austrian employees are subject to compulsory membership. The member fee is determined by law and is amounting to 0.5% of the members' gross wages or salaries (up to the social security payroll tax cap maximum). 560.000 - amongst others unemployed, persons on maternity (paternity) leave, community- and military service - of the 3.2 million members are exempt from subscription payment, but are entitled to all services provided by the Austrian Federal Chambers of Labour.

Herbert Tumpel
President

Werner Muhm
Director

Executive Summary

The AK welcomes the fact that the Commission is looking into the growing segment of payment cards and has raised a series of questions on secure payments at the point-of-sale (POS) and on the Internet.

Cardholders should be able to be confident that fees and services are set in their credit card agreement and not limited or undermined by merchants through restrictions.

We share the view of the Commission that there is room for improvement with respect to the transparency of charges. Many of the processes and innovations addressed in the Green Paper disregard the immediate interests of consumers. We cannot see how the co-badging project will bring any concrete benefits to consumers.

From the perspective of consumers, there is no reason why merchants (who accept cards for payment) should be given special leeway to set surcharges on certain forms of payment. Above all, cardholders should be able to be confident that fees and services are set in their credit card agreement and not limited or undermined by merchants (retailers, etc.) through restrictions - especially in the form of surcharges on certain payment methods.

The Commission has looked in great detail into multilateral interchange fees (MIF) and cites the "classic" business model for four-party card schemes, in which the interbank fees are paid by the merchant's PSP (the acquiring PSP) to the cardholder's PSP (the issuing PSP) for each card transaction.

The AK position in detail

There is an increased need for transparency in the case of transaction fees paid by cardholders directly, as well as foreign currency conversion fees for transactions and credit card payments in non-Euro currencies, which are not transparent and have been the source of many complaints received by our Chamber of Labour advice service.

MULTILATERAL INTERCHANGE FEES/ MIFS

Question 1: Under the same card scheme, MIFs can differ from one country to another, and for cross-border payments. Can this create problems in an integrated market? Do you think that differing terms and conditions in the card markets in different Member States reflect objective structural differences in these markets? Do you think that the application of different fees for domestic and cross-border payments could be objectively justified?

Multilateral interchange fees are not visible to credit card holders. According to the experience of Chamber of Labour, MIFs are neither discussed by merchants nor specifically mentioned in the general terms and conditions. As a result, MIFs are fees charged in a "black box".

Question 2: Is there a need to increase legal clarity on interchange fees? If so, how and by what means do you think this could be achieved?

In the case of credit cards and other payment cards (such as ATM cards), there are several cost items that can be passed on to the cardholder for using the card.

For example, when using a credit card for withdrawing cash at ATMs, there are charges set as a percentage of the withdrawn amount (3% in the Eurozone, plus a handling fee of 1 to 2% outside the Eurozone, depending on the credit card company), and at least very high minimum fees (in euros) between EUR 2.50 and EUR 4 (depending on the credit card). There is an increased need for transparency in the case of transaction fees paid by cardholders directly, as well as foreign currency conversion fees for transactions and credit card payments in non-Euro currencies, which are not transparent and have been the source of many complaints received by our Chamber of Labour advice service.

According to a survey conducted by the Chamber of Labour, the interest for partial payments (i.e. payment in monthly instalments) is not only relatively high (between 12.5% and 14% per annum), but also fixed and apparently not linked to the reference rate. The need for increased transparency applies to interest on partial payments as well.

Question 3: If you think that action on interchange fees is necessary, which issues should be covered and in which form? For example, lowering MIF levels, providing fee transparency and facilitating market access? Should three-party schemes be included? Should a distinction be drawn between consumer and commercial cards?

Cardholders (of credit cards as well as debit cards) pay an annual fee, which can vary depending on the credit card and scope of services included. According to a survey conducted by the Vienna Chamber of Labour, annual fees ranged in 2011 between EUR 18.17 (card without insurance protection) and EUR 500 (inclusive of 5 additional cards). In addition to the annual fee, there are additional charges (fees) for special services (collection fees, charges for cash withdrawals, processing fees for transactions outside the Eurozone, blocking charges) not covered by the (flat) annual fee.

The transparency of interchange fees may be useful for pricing and setting out contractual conditions for merchants, banks and credit card companies, but does not benefit cardholders.

The Vienna Chamber of Labour collects data on the additional fees each year and publishes the results to provide a cost comparison at www.arbeiterkammer.at. Apart from the considerable charges for cash withdrawals at ATMs (at least between EUR 2.50 and EUR 4.00), there is a noticeable difference in blocking charges applied, which at the time of the survey in May 2011 ranged between EUR 17 and EUR 40. If required, these fees are charged directly to cardholders, while the interchange fees are not a visible price component for cardholders.

The transparency of interchange fees may be useful for pricing and setting out contractual conditions for merchants, banks and credit card companies, but does not benefit cardholders.

CO-BADGING

Questions 6 and 7: What are the potential benefits and/or drawbacks of co-badging? Are there any potential restrictions to co-badging that are particularly problematic? If you can, please quantify the magnitude of the problem. Should restrictions on co-badging by existing schemes be addressed and, if so, in what form?

In its product policy, the Commission follows the co-badging approach, which means that different payment brands are combined on the same card or device. It is doubtful that it would be more useful for the cardholder if multiple brands were combined on the same card. It is not obvious from the idea of co-badging what the specifics should look like and whether cardholders will consider it an advantage to use one single card (but with multiple brands).

In Austria, the unbundling efforts of the credit card market led in 2007 to the two credit card market lead-

ers (Visa, Mastercard) expanding their respective product ranges and changing their company names. Both companies have since been offering the credit card (brand) of the main competitor and have thus become full-service credit card providers. The benefit of this supplier-side market trend for consumers is not clear, and according to the surveys conducted by the Chamber of Labour in previous years, it has resulted only occasionally in credit card price (fee) decreases. In contrast, some fees have become significantly higher (for example, the processing fee for transactions outside the Eurozone, reminder fees) and some annual fees have also increased. It has become even more difficult for consumers to associate a credit card brand with a particular credit card company.

The benefit of this supplier-side market trend for consumers is not clear, and according to the surveys conducted by the Chamber of Labour in previous years, it has resulted only occasionally in credit card price (fee) decreases.

The numerous credit cards issued by various banks as sub-licensees have made the market less transparent. It has also become more difficult for cardholders to evaluate the "product packages" that include insurance, because the product range offered by the various credit card companies in Austria has expanded considerably.

SEPARATING CARD SCHEMES AND CARD PAYMENT PROCESSING

The Commission sets some store by the separation of card schemes and card payment processing when it states that some card schemes have subsidiaries that process the transactions and are in a position to impose the use of these subsidiaries on scheme participants.

However, from the perspective of cardholders, card payment processing is only significant if there are obviously different billing periods (depending on the credit card) in which cardholders' credit card payments to merchants are debited.

These billing periods - presumably of different durations - have concrete effects for cardholders. The later an invoice amount - paid using a credit card to the merchant - is debited from the current account of the cardholder after the monthly statement has been issued, the greater the crediting effect.

A detailed breakdown of the billing period (length or number of days, start and end of the billing period) is usually not included in the general terms and conditions (GTC) of credit card companies. Instead, credit card companies advertise the crediting effect at best in very general terms with claims that the account will be debited "up to six weeks after payment". An average cardholder is hardly in a position to verify such advertising promises.

Therefore, it would be desirable if the cardholder had exact information (or if they had the option to receive such information under the general terms

and conditions) as to which payments (made by credit card) will be debited in the next monthly statement and/ or in the subsequent billing period. It would be desirable if an exact breakdown were provided in the pre-contractual information, or at least in the general terms and conditions (GTC). A consumer who chooses a credit card – as regards the billing period – will go for a credit card that offers the best crediting aspect. This is because it makes a difference whether the invoice paid with a credit card is debited from the current account 20 days later, or (as advertised) "up to 42 days" later. Credit card holders should be made aware when exactly the monthly bill will be debited from the current account. Bearing in mind this debit date, it is easier for cardholders to control current account liquidity, which could lead to consider-able cost savings.

It would be desirable if an exact breakdown were provided in the pre-contractual information, or at least in the general terms and conditions.

SEPA CREDIT CARDS

Question 12: What is your opinion on the content and market impact (products, prices, terms and conditions) of the SEPA Card Framework (SCF)?

Standardization efforts, especially security aspects, are of particular importance to cardholders. In previous years, the Chamber of Labour advice centres have received a number of complaints from cardholders reporting card abuse (mainly when on holiday). A common grievance in the past was that cards were apparently "copied" and then misused in the holiday destination. It cannot be the primary responsibility of the cardholder to ensure that credit card details are not copied.

Question 13: Is there a need to give institutions other than banks access to information on the availability of funds in bank accounts, with the agreement of the customer, and if so what limits would need to be placed on such information? Should action by public authorities be considered, and if so, what aspects should it cover and what form should it take?

Creditworthiness of the customer is checked as part of the credit card awarding process. Similarly, the card limit (for both credit and debit cards) is set depending on the customer's credit score. It is, however, not clear why any institution other than the card-issuing company should have access to information on the availability of funds in bank accounts.

TRANSPARENT AND COST-EFFECTIVE PRICING OF PAYMENT SERVICES FOR CONSUMERS, RETAILERS AND OTHER BUSINESSES

Question 15: Should merchants inform consumers about the fees they pay for the use of various payment instruments? Should payment service providers be obliged to inform

consumers of the Merchant Service Charge (MSC) charged/the MIF income received from customer transactions? Is this information relevant for consumers and does it influence their payment choices?

Consumers opt for (or against) a credit card on the basis of criteria such as its distribution (in a region), number of merchants, service and annual fees and the services included (such as insurance). The fees that the merchant is required to pay are based on the contract the merchant has with the credit card company.

A consumer who has entered into a credit card contract should not be concerned with (potential) surcharges or discounts that the merchant may set according to criteria that the consumer cannot control or understand at the point of making the payment.

A consumer who has entered into a credit card contract - mainly to use the card in return for a payment of an annual fee - should not, ideally, be concerned with (potential) surcharges or discounts that the merchant may set according to criteria that the consumer cannot control or understand at the point of making the payment (at the point of sale).

These pricing options would give merchants too much leeway, which is not in the best interest of the consumers. Surcharges, discounts, or even the simple reference to expensive disagio rates pose a systematic risk that the actual benefits to the account holder arising from the credit card agreement of his choice - the unrestricted use of the payment cards in stores displaying the credit card emblems - will be limited or slowly eroded. At the Chamber of Labour advice service, we see a number of cardholders complaining about merchants refusing to accept credit card payments citing that the disagio fees are too high or the minimum turnover threshold has not been reached, etc.

The question also arises as to how detailed information on disagio rates provided by merchants could be of any value to the cardholder (consumer). Rather, it can be assumed that, for example, the verbal information on a disagio for a credit card, "from 0.22%, the fixed fee per transaction is EUR 0.14", does not represent a suitable basis for making a decision for (or against) a particular payment card.

The normally educated consumer will not find the information on credit card X "incurring rates from 1.43% plus € 0.10 per transaction" (Source: Disagio information from credit card companies, March 2012) useful, because value-related percentages in combination with a minimum fee at the time of purchase or entering into a purchase agreement will not make any sense to him. At best, this information can be useful for distance selling, if consumers have sufficient time to consider and evaluate the offered pricing information on specific payment methods.

Question 17: Could changes in the card scheme and acquirer rules improve transpar-ency and facilitate

cost-effective pricing of payment services? Would such measures be effective on their own or would they require auxiliary measures? Would such changes require additional checks and balances or new measures concerning merchant-consumer relations, so that consumer rights are not affected? Should three-party schemes be included? Should a distinction be drawn between consumer and commercial cards? Are there specific requirements and implications for micro-payments?

Cardholders do not typically have any knowledge of the contracts between credit card issuers and merchants. From the perspective of the cardholder, it is important that consumers have legal certainty with respect to their credit card agreement and are aware of the fees and interest charged directly to them.

From the perspective of the cardholder, it is important that consumers have legal certainty with respect to their credit card agreement and are aware of the fees and interest charged directly to them.

Question 18: Do you agree that the use of common standards for card payments would be beneficial? What are the main loopholes, if any? Are there other specific aspects of card payments, other than the three mentioned here (A2I, T2A, certification), which would benefit from more standardisation?

Standardisation requirements are necessary for credit card payments, particularly as regards the use of PINs (Personal Identification Numbers), as well as the need for signature or the entry of a special code in the case of distance selling. For cardholders, there is uncertainty as to which security standards will be required in different countries and regions.

PAYMENT SECURITY

Question 25: Do you think that physical transactions, including those with EMV-compliant cards and proximity m-payments, are sufficiently secure? If not, what are the security loopholes and how could they be addressed?

We would like to refer to the recent OECD report on consumer protection for online and mobile payments (Committee on Consumer Policy DSTI/CP (2011)11/final dated 18/01/2012). In this respect, the particular challenges for the OECD include unfair billing, unfair business practices with deceptive or fraudulent intent, the protection of privacy, technical data security aspects, lack of interoperability, unclear rules regarding the rights and obligations of both contracting parties and the lack of dispute settlement mechanisms in case of conflict and insufficient education of consumers allowing them to protect themselves as service users against fraud and security risks.

With regard to the latter problem category, the OECD report draws attention primarily to common problems in practice. Online and mobile pay-

ments are carried out to an increasing extent by minors. As an example, the downloading of free apps with games targeted at children is cited, which encourages the purchase of paid apps.

Payment is often made via the mobile phone bill (WAP billing) or the credit card of the parents. Mobile phones that can be used to pay for transactions without the need for cash are often lost or stolen.

In its conclusion, the OECD paper shows that the problems that consumers have when using electronic means of payment for Internet transactions are extremely diverse. From AK's perspective, the legal framework and the payment terms offer the consumer less and less security in the light of the developments in the e- and m-commerce services, because, among other reasons:

The legal framework and the payment terms offer the consumer less and less security in the light of the developments in the e- and m-commerce services, because, among other reasons:

- the protection of minors is inadequate (no suitable age verification procedure, etc.)
- There is currently no effective control of abuse on the supply side, especially with respect to dishonest payees (Internet services, apps offers, WAP services, etc.). As a result of an increase in such providers who have fraudulent intentions with respect to consumer purchases over the Internet, pretend that a service is free when it is not, intentionally do not provide a service, etc. it is imperative to include special security elements in the payment process, which would at least make abuse more difficult.
- in the event of unfair or fraudulent conduct there is not enough clarity about the responsibility of the payment service providers (reversal duties; evaluation of the reliability of the payee, etc.)
- the mobile phone as a payment method is extremely risk-prone (abuse of mobile phones through access by unauthorized third parties in the case of theft, for example; lack of protection of the operating system of the mobile phone through filtering software and firewalls; settlement via the mobile phone bill or mobile payment solutions (such as Paybox in Austria) without basic security standards being implemented, such as payment authorisation using PIN codes, far too little awareness on the part of users that their mobile phone can be used as a payment instrument, etc.)

Question 26: Are additional security requirements (e.g. two-factor authentication or the use of secure payment protocols) required for remote payments (with cards, e-payments or m-payments)? If so, what

specific approaches/technologies are most effective?

Yes they are. With regard to the question of whether two-factor authentication would represent a step forward, the AK has always pointed out that there are currently payment methods that are not protected from abuse by even a simple code. Payments via mobile phone bill, such as WAP billing, are rightly considered to be especially prone to abuse. The service provider identifies the user through a unique IP address that he then forwards to the mobile operator who collects the amount for the ordered service. The affected customer will often find out about a claim by a rogue provider only when he reviews his mobile phone bill.

There is also a lack of transparency and state-of-the art security in the cooperation between mobile operators and m-payment providers.

There is also a lack of transparency and state-of-the art security in the co-operation between mobile operators and m-payment providers. When acquiring a new mobile phone, Austrian mobile customers had the m-payment function "Paybox" automatically unlocked without their knowledge. When the mobile phone was stolen it happened very often that the customer account was dishonestly debited, as payment transactions over the Internet could be made using a simple SMS order. There was no minimum protection by using a PIN code - to make it more convenient for the user, according to the operators.

Against this background, it should be demanded that mobile payments are never automatically agreed as part of a mobile phone contract. Such functions may only be enabled at the express request of the customer. The customer must be informed prior to releasing any material contractual details: Security aspects, sharing of responsibility in the case of abuse, service blocking options, maximum amount limits for daily and monthly usage, authorisation requirement for payment transactions, who stores which customer data in the service provider chain between mobile operators, payment service providers, payees, etc.

The greater the risk the consumer is exposed to (concluding a payment service contract with unverified Internet service providers, amount of payment transactions is not only limited to micro-payments, etc.), the more security measures should be demanded. Alternatively, the payment service can assume general responsibility for cases of abuse and initiate a refund following a cursory examination.

Credit card issuers currently rely primarily on rapid settlement of conflicts by issuing credits for Internet payments, and the majority do not require customer authorisation using a security code and PIN (although there are some online retailers who already require this secure customer identification).

A decisive factor for consumers is also the careful handling of their loyalty cards. While the established banking institutions tend to observe privacy legislation, this is not the case with other payment service providers that are not subject to a rigorous certification process in the country of establishment or provide cross-border services from a third country. Their reliability and integrity in dealing with customer data may be questionable in many cases, so their access to consumer bank account data should be prevented by law. Moreover, a certification of data applications (limitation to data absolutely necessary for the fulfilment of the contract, no disclosure to third parties, deletion routines, technical and organisational data security concepts, seamless logging of events) would be required, as would continuous and effective monitoring of their business activity.

An additional specific legal framework would be desirable. The general provisions of the distance selling legislation, E-Commerce Act and data protection legislation are not sufficient.

Question 27: Should payment security be underpinned by a regulatory framework, potentially in connection with other digital authentication initiatives? Which categories of market actors should be subject to such a framework?

Yes, an additional specific legal framework would be desirable. The general provisions of the distance selling legislation, E-Commerce Act and data protection legislation are not sufficient. Due to the multi-party relationships involved in service provision, the scope of personal data processed, the recipients and the responsibility for safe data processing are urgently in need of regulation.

At present, in the case of electronic services, the interaction between payees, payment services, mobile operators, etc. is quite inconsistent and not transparent for the consumer, and liability is not clearly defined. This applies to the area of privacy protection (who fulfils which customer obligations with respect to the individual data applications), as well as the guarantee of data security (even in the case of an encrypted data transmission, who ensures that the same level of safety is maintained at the transfer interface, security problems as a result of an international data transfer involving various service providers in third countries without an adequate level of security, etc.), and also to cases of misuse (who investigates the incident, will be eligible for a free credit, etc.).

Question 28: What are the most appropriate mechanisms to ensure the protection of personal data and compliance with the legal and technical requirements laid down by EU law?

Any data application used by a payment service should be subject to a prior check by the competent registration authority, which may impose restrictions.

In accordance with the Data Protection Directive 95/46/EC or the proposed Data Protection Regulation, customers must be informed about the data types used, their purpose, recipients, time of deletion, etc. prior to using the payment services. The information that is currently provided tends to be very poor, calling for more stringent industry supervision.

The payment service provider should be required to conduct a risk assessment as regards how this data might be misused within the company and externally and submit it to data protection supervisory authorities prior to commencing operations.

The payment service provider should be required - in line with the approach taken by the proposed Data Protection Regulation - to conduct a risk assessment as regards how this data might be misused within the company and externally (data manipulation through hacking attacks, abuse by unscrupulous payees, etc.) and submit it to data protection supervisory authorities prior to commencing operations. Providers within the EU should be urged to obtain EuroPriSe - the European Privacy Seal. The use of service providers from third countries without an adequate level of security should not be permitted even if standard contract terms on data security have been agreed.

Should you have any further questions please do not hesitate to contact

Mr Christian Prantner
Tel: +43-(0)1-50165/2511
e-mail: christian.prantner@akwien.at

Mrs Daniela Zimmer
Tel: +43-(0)1-50165/2722
e-mail: daniela.zimmer@akwien.at

as well as

Mr Frank Ey
Tel: 0032/2/2306254
e-mail: frank.ey@akeuropa.eu
at our AK office in Brussels.

Bundesarbeitskammer Österreich
Prinz-Eugen-Strasse, 20-22
A-1040 Vienna, Austria
T +43 (0) 1 501 65-0
F +43 (0) 1 501 65-0

AK EUROPA
Permanent Representation to the EU
Avenue de Cortenbergh, 30
B-1040 Brussels, Belgium
T +32 (0) 2 230 62 54
F +32 (0) 2 230 29 73