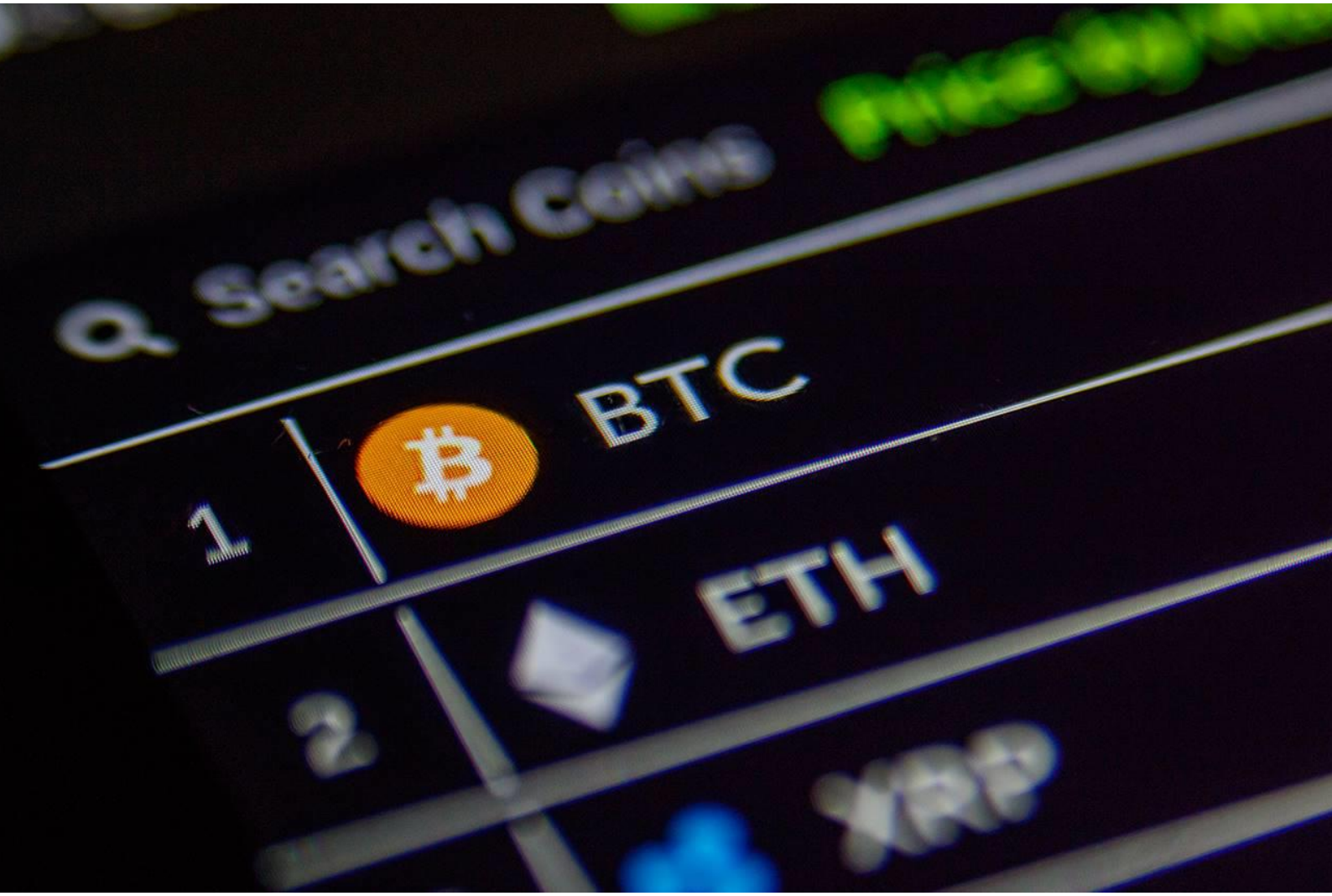
ALLEN & OVERY

Payments & FinTech

News



Contents

Hot Topic

Final Report on draft RTS amending Commission Delegated Regulation (EU) 2018/389 published

On 5 April 2022, the EBA published its final Report on the amendment of its regulatory technical standards on strong customer authentication and secure communication under the Payment Services Directive (the 'RTS on SCA&CSC'). Most notably, the changes introduce a new mandatory exemption to SCA that will require account servicing payment service providers ('ASPSPs') not to apply SCA when customers use an account information service provider ('AISP') to access their payment account information, provided certain conditions are met, while limiting the scope of the existing voluntary exemption to SCA in Article 10 of the RTS on SCA&CSC to instances where the customer accesses the account information directly. In the following, we will briefly explain the scope of the SCA and the current exemption before discussing the proposed amendments to the RTS on SCA&CSC and their respective backgrounds, also taking into account the concerns raised in the public consultation and the EBA's responses to those concerns.

1. SCA and current AISP exemption

Article 97 of Directive (EU) 2015/2366 ('PSD2') requires payment service providers to apply SCA each time a payment service user accesses its payment account online, initiates an electronic payment transaction or carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

At the same time, Article 98(1) of PSD2 mandated the EBA to develop regulatory technical standards specifying the requirements of SCA and the exemptions from the application of SCA. In fulfilment of this mandate, the EBA developed the RTS on SCA&CSC, which entered into force as an EU Delegated Regulation on 14 September 2019.

The RTS on SCA&CSC contain nine exemptions to SCA, one of which (in Article 10) concerns the access to payment account information. Said exemption allows ASPSPs not to apply SCA where the payment services user accesses its payment account information, provided that certain conditions are met, namely:

(i) the information accessed is limited only to the balance of the account and/or the recent transaction history,

(ii) no sensitive payment data are disclosed; and

(iii) SCA is applied when the account information is accessed for the first time, and at least every 90 days after that.

The exemption applies both when the PSU accesses the account directly and through an AISP.

The EBA introduced this exemption because, without it, the requirements set out in the PSD2 to apply SCA for every single access would have undermined the business viability of account information services, which the PSD2 explicitly sought to promote as a new innovative service in the EU.

2. Background to the draft RTS

The current exemption to SCA in Article 10, as well as all other exemptions to SCA in the RTS on SCA&CSC, is voluntary in nature. This means that ASPSPs are allowed, but not obliged, to use the exemption and at any time could choose to apply SCA to the actions falling within the scope of the exemption. This approach followed the consideration that the payment service provider applying SCA is the one that issues the personalised security credentials, namely the ASPSP. Accordingly, it is the ASPSP that is obliged under PSD2 to perform SCA and bears the liability if it fails to protect the security of the payment service user's data and funds. For these reasons, the RTS on SCA&CSC do not restrict ASPSPs from applying SCA even where an exemption can be used.

According to the EBA, however, the experience gained in the first years of the application of the RTS on SCA&CSC has shown that, with regard to this particular exemption in Article 10, the voluntary nature of the exemption has led to very divergent practices in its application, with some ASPSPs requesting SCA every 90 days, others at shorter time intervals, while a third group of ASPSPs have not applied the exemption at all and request SCA for every account access.

The inconsistent application of the exemption and the frequent application of SCA have thus led to undesirable friction for customers and to a negative impact on AISPs' services. This has been particularly the case where the customer uses the services of an AISP to aggregate multiple accounts held with different account providers and has to perform multiple SCAs, one with each ASPSP, in order to be able to continue using the AISP's services.

Moreover, the EBA states that the application of SCA for every single access where the ASPSP does not apply the exemption is limiting certain use cases that rely on the AISP's ability to access the data without the customer's involvement (as examples the EBA mentions personal finance management services and cloud accounting services). This would limit the customers' ability to make use of such services and the AISPs' ability to offer its services in the EU single market, contrary to the PSD2 objectives of facilitating innovation and enhancing competition.

Having assessed these issues, the EBA decided to amend the RTS on SCA&CSC in order to bring further harmonisation in the application of the exemption, when the access to account information is done through an AISP. Against this background, the EBA decided to propose a targeted amendment to the RTS on SCA&CSC, in order to:

- introduce a new mandatory exemption to SCA, only for the specific case when access is through an AISP and only if certain conditions are met (the 'AISP Exemption'), while limiting the scope of the voluntary exemption in Article 10 of the RTS on SCA&CSC to the case where the customer accesses the account information directly; and
- extend the timeline for the renewal of SCA from every 90 days to every 180 days, both where the information is accessed through an AISP or directly by the customer.

In addition, the EBA has also introduced other less substantive amendments to the draft amending RTS, which are explained in the following section.

3. Amendments to RTS on SCA&CSC in detail

New AISP Exemption

The draft amending RTS introduce a new Article 10a to the RTS on SCA&CSC. According to Article 10a(1) ASPSPs shall not apply SCA, subject to compliance with the requirements laid down in Article 10a(2), where a payment service user is accessing its payment account online through an AISP, provided that access is limited to either or both of the following items online without disclosure of sensitive payment data:

(a) the balance of one or more designated payment accounts;

(b) the payment transactions executed in the last 90 days through one or more designated payment accounts.

In contrast, Article 10a(2) provides that ASPSPs shall apply SCA where either of the following conditions is met:

(a) the payment service user is accessing online the account information for the first time through the AISP;

(b) more than 180 days have elapsed since the last time the payment service user accessed online the account information through the ASPSP and SCA was applied.

By way of derogation from Article 10a(1), Article 10a(3) allows ASPSPs to apply SCA where a payment service user is accessing its payment account online through an AISP and the ASPSP has objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account. In such a case, the ASPSP shall document and duly justify to its national competent authority, upon request, the reasons for applying SCA.

A primary concern raised in the consultation was that a mandatory exemption would remove a layer of security and may lead to increased security risks, as it would not allow ASPSPs to carry out suitable risk and fraud management or apply an appropriate protection level to their customers. It was argued that fraudsters may undermine the ASPSP's security policy by using AISPs for getting access to customers' accounts.

While the EBA acknowledged the importance of the security of customer's funds and data, it is of the view that the proposed amendments to the RTS strike an appropriate balance between the PSD2 objective of enhancing security, on the one hand, and the innovation and competition enhancing objectives of PSD2, on the other. Furthermore, the EBA is confident that the conditions and safeguards introduced in Article 10a(1), (2) and (3) to accompany the new AISP Exemption mitigate the risk of unauthorised or fraudulent access and make the exemption compatible with the level of risk involved.

In addition, the EBA stresses that AISPs are regulated and supervised entities that are subject to security and data protection requirements set out in the PSD2 and other legislation, such as the EU General Data Protection Regulation, which would reduce the risk of any data breaches in this context significantly.

Extension of SCA renewal frequency

The draft amending RTS extend the timeline for the renewal of SCA from 90 to 180 days, regardless of whether the payment services user accesses its payment account online directly or through an AISP. Accordingly, ASPSPs shall not be exempted

from the application of SCA where, amongst others, more than 180 days have elapsed since the last time the payment service user accessed online the account information directly or through an AISP and SCA was applied.

In the consultation, some respondents raised concerns that the proposed 180-day timeline for the renewal of SCA may increase the risk of unauthorised or fraudulent access during the 180-day period and preferred to retain the current 90-day period. By contrast, other respondents shared the opposite view and suggested increasing this timeline to 1 year or more, which would be more suitable given the low fraud risk associated with account information services and the safeguards accompanying the new AISP Exemption.

However, the EBA is of the view that the obligation to renew SCA every 180 days, combined with the ability of ASPSPs to revert at any time to SCA, where they have objective reasons to suspect an attempted unauthorised or fraudulent access, as well as the safeguards accompanying the new AISP Exemption, strike a good balance between the PSD2 objective of ensuring security, on the one hand, and the innovation and competition enhancing objectives of the PSD2, on the other.

Implementation period

The draft amending RTS shall be directly applicable in all EU Member States seven months after its entry into force. Moreover, Article 2 of the draft amending RTS provides that ASPSP shall make available to third-party payment service providers ('TPPs') any changes to the technical specifications of their interfaces made to comply with the AISP Exemption not less than 2 months before such changes are implemented.

The draft amending RTS proposed in the consultation paper included an implementation period of six months after their publication in the Official Journal, while ASPSPs had to make available to the AISPs the changes to the technical specifications of their interfaces one month prior to the overall implementation. Both of these periods were perceived as too short by a number of respondents in the consultation. The six-month implementation period would not suffice for ASPSPs to implement the required changes into their systems. The one-month period for making available the changes ahead of implementation, on the other hand, would not allow the AISPs to understand the technical specifications of all the ASPSPs to which they are connected and to make the necessary changes to their systems.

Therefore, the EBA has decided to extend these time periods from six to seven months and from one to two months, respectively. Accordingly, ASPSPs will have five months to make available to TPPs the documentation with the changes to the technical specifications of its interfaces and allow TPPs to test them in the testing facility, and seven months to implement those changes in the production environment.

According to the EBA, this should give sufficient time to both ASPSPs and AISPs to implement the necessary changes in their systems to comply with the AISP Exemption.

Additional minor clarifications

The EBA has introduced some introduced other less substantive amendments to the draft amending RTS, addressing further concerns that were raised in the consultation, including the following:

(i) Pursuant to Article 10a(4), ASPSPs that offer a dedicated interface and have not received an exemption from the requirement to set up the contingency mechanism referred to in Article 33(4) of the RTS on SCA&CSC are not required to implement the AISP Exemption in their direct customer interfaces for the purpose of the contingency mechanism, if they do not apply the exemption in Article 10 of the RTS on SCA&CSC in the direct interface used for authentication and communication with their payment service users.

(ii) Article 3(3) of the draft amending RTS provides that ASPSPs that applied the exemption in Article 10 of the RTS on SCA&CSC prior to the application date of the amending RTS shall be allowed to continue applying that exemption up to 90 days from the last time SCA was applied. This is however without prejudice to the application of the mandatory exemption in Article 10a of the draft amending RTS for new access requests received through an AISP, for which SCA is applied, starting with the application date of the amending RTS.

4. Next steps

The draft amending RTS will be submitted to the Commission for endorsement following which it will be subject to scrutiny by the European Parliament and the Council before being published in the Official Journal.

The amending RTS will enter into force on the twentieth day following that of its publication in the Official Journal and shall apply seven months after entry into force. The amending RTS will be binding in its entirety and directly applicable in all EU Member States.

As regards the regulatory practice in Germany, due to the binding nature of the amending RTS, BaFin will have to apply them regardless of whether or not they agree with the envisaged changes made by the EBA.

ASPSPs should consider how to implement the necessary changes in their systems to comply with the mandatory AISP Exemption. In addition ASPSPs should carefully assess whether any amendments to the terms and conditions with the payment services user are required (in line with Article 54 of PSD2) and duly communicate and explain these changes to them before the application date of the amending RTS.

Regulatory Updates

Payments

EU

EBA: Final report on draft RTS amending Commission Delegated Regulation (EU) 2018/389

The EBA has published its final report on the amendment of its RTS on the exemption to strong customer authentication ('SCA') and secure communication for account access under PSD2. The changes:

(i) introduce a new mandatory exemption to SCA that will require account providers not to apply SCA when customers use an account information service providers (AISP) to access their payment account information, provided certain conditions are met. The amendment aims to reduce frictions for customers using such services and to mitigate the impact that the frequent application of SCA and the inconsistent application of the current exemption have on AISPs' services;

(ii) limit the scope of the voluntary exemption in Article 10 RTS to instances where the customer accesses the account information directly; and

(iii) extend the timeline for the renewal of SCA from every 90 days to every 180 days, both when the information is accessed through an AISP or directly by the customer.

In light of comments received, the EBA introduced some changes to the draft amending RTS. In particular, the EBA extended the timeline for ASPSPs to make available to AISPs the changes to their interfaces from 1 month to 2 months before the implementation of these changes and extended the overall implementation period from 6 months to 7 months after the publication of the amending RTS in the OJ. The EBA also introduced some additional clarifications on the application of the mandatory exemption.

The draft amending RTS will be submitted to the Commission for endorsement following which it will be subject to scrutiny by the European Parliament and the Council before being published in the Official Journal of the European Union. The amending RTS will apply 7 months after entry into force.

Date of publication: 05/04/2022

For details on EBA's final report, see our 'Hot Topic' section above.

FinTech/Digital finance

EU

EP: Adoption of Regulation on pilot regime for market infrastructures based on DLT at first reading

The European Parliament ('EP') has adopted its position on the European Commission's ('EC') legislative proposal for a Regulation on a pilot regime for market infrastructures based on DLT at first reading. Amendments to the EC's proposal among other things, limit the financial instruments admitted to trading on, or settled by, a DLT market infrastructure, mainly in terms of market capitalisation (shares), issuance size (bonds) or issuance volume (exchange-traded funds). The EP, in a background information document published on 21 March state that whilst its amendments set lower thresholds for financial instruments admitted to trading on, or settlement by, a DLT market infrastructure, the limits set in the provisional political agreement reached between the Council and Parliament on 24 November 2021 are more munificent. The Council will now need to adopt the proposed Regulation, which will enter into force 20 days after it is published in the OJ and will apply nine months after the date it has entered into force.

Date of publication: 24/03/2022

EU

ECON: ECON: Adoption of report on Markets in Cryptoassets Regulation (MiCAR)

The Economic and Monetary Affairs Committee (ECON) of the EP has adopted its negotiating position on the proposed Markets in Cryptoassets Regulation (MiCAR). Key provisions agreed for those issuing and trading cryptoassets cover transparency, disclosure, authorisation and supervision of transactions. The agreed text also includes measures against market manipulation and to prevent money laundering, terrorist financing and other criminal activities. ECON focuses on:

(i) *climate change*. To reduce the high carbon footprint of crypto-currencies, ECON asks the EC to present a legislative proposal to include in the EU taxonomy for sustainable activities any cryptoasset mining activities that contribute substantially to climate change, by 1 January 2025. ECON also calls on the EC to work on legislation addressing issues arising from other sectors that consume energy resources that are not climate-friendly, such as the video games and entertainment industry, as well as datacentres; and

(ii) *supervision*. ECON wants ESMA to supervise the issuance of asset-referenced tokens, whereas the EBA would be in charge of supervising electronic money tokens. In a next step, the EP will enter into negotiations with EU governments on the final shape of the bill.

Date of publication: 14/03/2021

EU

EC: Launch of EU Digital Finance Platform

The EC has launched an EU Digital Finance Platform, consisting of a Digital Finance Observatory and a European Forum for Innovation Facilitators Gateway. The platform is intended to be a collaborative space bringing together industry and public authorities to support innovation in the EU's financial system and help work towards a true Single Market in digital finance.

The Digital Finance Observatory features an interactive mapping of the EU's fintech sector, an overview of the latest policy developments and research, events and calls to action.

The Gateway shall provide innovative firms with access to national supervisors, including to cross-border testing with multiple authorities. This part of the Platform also offers information on how to contact relevant national authorities and find out about national licensing requirements, as well as

updates on the work of the European Forum for Innovation Facilitators.

Date of publication: 08/04/2021

EU

EC: Targeted consultation and call for evidence on a digital euro

The EC has launched a targeted consultation on the digital euro, following its 2020 public consultation, in order to collect further information on expected impacts on key industries (financial intermediation, payment services, merchants), users (consumer associations, retailers' associations), chambers of commerce and other stakeholders in international trade.

The consultation focuses on:

(i) users' needs and expectations for a digital euro;

(ii) the digital euro's role for the EU's retail payments and the digital economy;

(iii) making the digital euro available for retail use while continuing to safeguard the legal tender status of euro cash;

(iv) the digital euro's impact on the financial sector and the financial stability;

(v) application of AML-CFT rules;

(vi) privacy and data protection aspects; and

(vii) international payments.

The EC has also launched an accompanying call for evidence for an impact assessment on the digital euro. The call for evidence notes that the EC adoption of a potential Regulation on the digital euro is planned for Q1 2023.

Date of publication: 05/04/2022

EU

Council: Three-column table to commence trilogue on the MiCA Regulation

The Council of the EU published a three-column table comparing the negotiating positions taken by the EC, the Council of the EU and the EP on the proposal for a Regulation on markets in crypto assets (MiCAR), as trilogues commence.

Date of publication: 01/04/2022

News from the Courts

Payments

Germany

Higher Regional Court of Frankfurt am Main, ruling of 30/09/2021 – 6 U 68/20 (Prima facie evidence in case of lost debit card)

Background of the case is a dispute between the defendant bank and its customer. The bank provided the customer with a debit card and allowed her to make cash withdrawals from ATMs using the PIN provided to her. On September 2018, between 11 am and 12 pm, three cash withdrawals amounting to €990 were made from an ATM, which were debited from the customer's account. At around 5 pm, the customer had the card blocked; it had been stolen from her. The customer demanded that the bank reimburse the amounts debited, which the bank refused to do on the grounds that the cash withdrawal had been made with the original debit card and the PIN had been entered, so that it could be assumed on the basis of prima facie evidence that the user of the debit card had been aware of the PIN and that it had therefore not been kept sufficiently secret by the customer. In April 2019, the plaintiff, a consumer protection association, unsuccessfully issued a warning to the defendant. It considers the fact that the defendant invokes the rules of prima facie evidence to be knowingly unfairly misleading. The Regional Court dismissed the action. The plaintiff's appeal is directed against the ruling of the Regional Court, in which he continues to pursue his claims at first instance.

According to the plaintiff, the fact that the bank refused to reimburse the withdrawn funds by stating that the customer had not kept the PIN sufficiently secret, because cash could not be withdrawn from the debit card without knowledge of the PIN, constitutes a misleading commercial practice within the meaning of Sec. 5(1) no. 7 of the German Unfair Competition Act (*Gesetz gegen unlauteren Wettbewerb*), i.e. a commercial practice that contains false statements or other information suited to deception regarding the rights of consumers, particularly those based on promised guarantees or warranty rights in the event of impaired performance. In this respect, the plaintiff referred to Sec. 675w sent. 3 of the German Civil Code (*Bürgerliches Gesetzbuch* – 'BGB'), which provides that the initiation of a payment transaction using a payment instrument, including authentication by the payment service provider, is not necessarily sufficient in itself to prove that the payer breached one or several conditions for the issuance and use of the payment instrument by gross negligence. Rather, the payment service provider is obliged under Sec. 675w sent. 4 BGB to present supporting evidence if it wants to prove gross negligence on the part of the payer.

The Higher Regional Court of Frankfurt am Main (*Oberlandesgericht Frankfurt am Main* – 'OLG Frankfurt') dismissed the dismissed the appeal. According to the court, the defendant bank did not violate Sec. 675w sent. 4 BGB. This sentence has been added to Sec. 675w BGB with effect from 13 January 2018 in implementation of Article 72 of PSD2. The meaning of Sec. 675w sent. 3 and sent. 4 BGB has been the subject to discussion in case law and legal doctrine since then.

Before the introduction of Sec. 675w BGB in 2009 it was acknowledged that in the case of payments where it could be proven that the original card and PIN had been properly used to initiate the payment transaction, there was prima facie evidence that the withdrawal or payment had been made by the customer himself or had at least been facilitated by him, since only he knew the secret number. The customer's statement that he had not made the withdrawal or payment himself and that he had lost the card did not refute the evidence. The prima facie

evidence was that the PIN was written on the card or kept in the immediate vicinity, i.e. that the payer had acted with gross negligence.

Following the introduction of Sec. 675w sent. 3 BGB, it was disputed whether the provision precluded the application of prima facie evidence, since according to it (among other things) the use of the debit card and the authentication as a result of entering the PIN alone is not necessarily (sufficient) to prove that the payer intentionally or grossly negligently violated the conditions for the use of the card. In 2016, the German Federal Supreme Court (*Bundesgerichtshof* – 'BGH') has ruled that Sec. 675w sent. 3 BGB does not prevent the application of prima facie evidence, but rather imposes special requirements on its design. Accordingly, for the application of the principles of prima facie evidence in payment services law in proving authorisation by a payment instrument, the correct recording of the use of this instrument alone is not sufficient. Rather, its general practical security and compliance with the security procedure must be established in the specific individual case.

According to the OLG Frankfurt, the principles on prima facie evidence must be adhered to even after the insertion of sent. 4 in Sec. 675w BGB. This is also supported by the mentioned BGH ruling, which was issued before the entry into force of Sec. 675w sent. 4 BGB, but after the adoption of PSD2. The supporting evidence in the sense of this provision can thus also consist of proving the conditions for the applicability of prima facie evidence, i.e. demonstrating the practical impregnability of the security features of payment cards.

The defendant bank argued that the PIN could neither be read out of the magnetic strip nor determined by manipulating the card. The stolen debit card was equipped with the latest chip technology V-PAY; V-PAY was a purely chip-based procedure in which all transactions were processed via an EMV chip, which effectively prevented card forgery and manipulation. An expert appointed by the court also came to the conclusion that it is practically impossible to copy a bank card with an EMV chip, which is due to the physical security features that are used directly on the chip and would make it very difficult to open and understand the circuitry of the chip without destroying it. So far, this has not been possible even under laboratory conditions.

By referring to the use of this chip technology, the defendant bank demonstrated to the conviction of the court the practical impregnability of the payment card's security features, thus proving the conditions for the applicability of prima facie evidence and thus satisfying the requirements of Sec. 675w sent. 4 BGB.

FinTech / Digital Finance

Germany

Regional Court of Munich I, ruling of 28/09/2021 – 33 O 15655/20 (Inadmissibility of a comparison portal for payment accounts with coverage of less than half of the accounts offered in Germany)

The plaintiff, a consumer protection association, asserts claims for injunctive relief under competition law against the defendant, which belongs to the Check24 group. The defendant operates a website for website comparing fees charged by payment service providers for services linked to payment accounts. The payment account offers displayed on the comparison website included three payment account offers by one credit institution, two payment account offers each by 14 credit institutions and only one payment account offer each by 541 credit institutions. The comparison website contained the following statement: "the comparison contains a wide range of direct, branch and regional banks, but does not offer a complete market overview". The plaintiff issued a warning to the defendant for non-compliance with the requirements of Sec. 18 no. 6 of the German Payment Accounts Act (*Zahlungskontengesetz* – 'ZKG') and Sec. 9 of the German Comparison Websites Ordinance (*Vergleichswebsitesverordnung* – VglWebV), amongst others, and demanded that the defendant issue a cease-and-desist declaration with a penalty clause. In support of its claim, the plaintiff argues that 1,717 credit institutions exist in Germany, of which approx. 1,300 credit institutions offer a payment account. However, on the defendant's comparison website only 572 payment account offers are displayed, which not only compares less than half of the payment accounts offered in Germany, but also have a market coverage of less than 50% with regard to the number of credit institutions offering payment accounts and thus does not cover a significant part of the market as required by Sec. 18 no. 6 ZKG. The defendant did not issue a cease-and-desist declaration. The plaintiff is now pursuing his claim with an action for an injunction against the defendant under the German Unfair Competition Act (*Gesetz gegen unlauteren Wettbewerb*).

The Regional Court of Munich I has granted the injunction. According to the court, the defendant's comparison website does not meet the requirements of Sec. 18 no. 6 ZKG and Sec. 9 VglWebV for the following reasons:

Under Article 7(1) of the EU Payment Accounts Directive ('PAD'), which is implemented in Germany by Sec. 16 et seqq. ZKG, Member States are required to ensure that consumers have access, free of charge, to at least one website comparing fees charged by payment service providers at national level for payment account services. The comparison website should "include a broad range of payment account offers covering a significant part of the market" (cf. Article 7(3)(f) PAD). In implementing these requirements, Sec. 18 no. 6 ZKG stipulates that a comparison website must contain sufficient payment account offers to cover a substantial part of the German market; Sec. 9 VglWebV further specifies that the market overview must contain a balanced number of offers from each banking group.

It is not sufficient, as happened on the defendant's comparison website, to display only one payment account offer for 90% of the credit institutions represented on the comparison website, although the majority of banks have more than one payment account model in their offer. Rather, Sec. 18 no. 6 ZKG requires – in accordance with Article 7(3)(f) PAD – that the comparison website must contain sufficient payment account offers to cover a substantial part of the German market. Consequently, the presentation of a balanced number of offers from each banking group is not sufficient, but it is additionally required that a "broad range of payment account offers" per represented credit institution are presented. Only in this way can the goal of providing consumers with the most complete and comprehensive information possible be met. As of 31 December 2019, approx. 1,300

credit institutions held payment accounts for consumers. In contrast, the defendant's comparison website contained (only) offers from around 560 credit institutions. Accordingly, less than 50% of the credit institutions offering payment accounts for consumers were compared on the website. The small number of credit institutions compared, cannot therefore guarantee the regional coverage of the German banking landscape required by Sec. 18 no. 6 ZKG, Sec. 9 VglWebV. It therefore does not meet the legal requirements.

The statement provided for in Sec. 18 no. 6 ZKG (Article 7(3)(f) PAD) and reproduced by the defendant on its website that the information offered does not constitute a complete market overview does not exempt the defendant from the requirement to present sufficient payment account offers so that a substantial part of the German market is covered. This is because the requirements contained in Sec. 18 no. 6 ZKG apply cumulatively and not alternatively.

Contacts

Payments and FinTech Regulatory

Dr Alexander Behrens
Partner
Tel +49 69 2648 5730
alexander.behrens@allenovery.com

Woldemar Häring
Counsel
Tel +49 69 2648 5541
woldemar.haering@allenovery.com

Kai Schadtle
Senior Associate
Tel +49 69 2648 5768
kai.schadtle@allenovery.com

Lukas Wagner
Associate
Tel +49 69 2648 5906
lukas.wagner@allenovery.com

Niklas Germayer
Associate
Tel +49 69 2648 5973
niklas.germayer@allenovery.com

Betül Kohlhäufl
Associate
Tel +49 69 2648 5788
betuel.kohlhaeufl@allenovery.com

Lisa Huber
Professional Support Lawyer
Tel +49 69 2648 5467
lisa.huber@allenovery.com

Derivatives and Structured Finance, Debt Capital Markets

Martin Scharnke
Head of ICM Germany
Tel +49 69 2648 5835
martin.scharnke@allenovery.com

Amar Memic
Senior Associate
Tel +49 69 2648 5811
amar.memic@allenovery.com

Sascha Fröhlig
Associate
Tel +49 69 2648 5463
sascha.froehlig@allenovery.com

ECB in focus

ECB in focus is our blog dedicated to the banking supervisory activities of the European Central Bank (ECB). We report on key developments in European banking regulation led by the ECB as part of the Single Supervisory Mechanism.

The blog features views and commentary from members of Allen & Overy's market-leading **German financial services regulation** practice.

For enquiries regarding Allen & Overy's ECB in focus blog, please **contact us**.

Featured posts

ECB REPORTS ON SANCTIONING ACTIVITY FOR 2020

ECB ENCOURAGES EUROPEAN CROSS-BORDER BANKING INTEGRATION

EBA PEER REVIEW REPORT ON ESA'S GUIDELINES ON QUALIFYING HOLDINGS

For more information, please contact:

Frankfurt

Allen & Overy LLP
Bockenheimer Landstraße 2
60306 Frankfurt am Main
Germany

Tel +49 69 2648 5000
Fax +49 69 2648 5800

Global presence

Allen & Overy is an international legal practice with approximately 5,600 people, including some 580 partners, working in more than 40 offices worldwide. A current list of Allen & Overy offices is available at **allenovery.com/global/global_coverage**.

Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. Allen & Overy LLP is a limited liability partnership registered in England and Wales with registered number OC306763. Allen & Overy LLP is authorised and regulated by the Solicitors Regulation Authority of England and Wales.

The term partner is used to refer to a member of Allen & Overy LLP or an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP's affiliated undertakings. A list of the members of Allen & Overy LLP and of the non-members who are designated as partners is open to inspection at our registered office at One Bishops Square, London E1 6AD.