60 YEARS YOUNG YEARS STRONG

BEUC The European Consumer Organisation

The Consumer Voice in Europe

REVIEW OF THE PAYMENT SERVICES DIRECTIVE 2

BEUC recommendations

Contact: Anna Martin – financialservices@beuc.eu

BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2022-118 – 21/11/2022

Why it matters to consumers

Every consumer makes one or more payment transactions almost every day. However, the way consumers pay is changing. Moving from coins, notes, cheques, cards and wire transfers, payments increasingly take place online and via mobile phones. This allows for more payment options and more convenience but also brings new challenges to keep consumers' bank accounts, payment cards and e-wallets secure. This paper addresses how a revised Payment Services Directive 2 (PSD2) needs to be updated to ensure a high-level of consumer protection in these changing realities.

Summary

The digitalisation of payment transactions brings convenience, but consumers cannot fully trust in the use of online and mobile payments or when interacting with new payment service providers. That is because the following problems can occur:

- There is a multitude of actors operating in the payment sector with various statutes and roles who are subject to different legislative frameworks (e.g. PSD2, e-Money Directive, SEPA – the Single Euro Payments Area). For consumers this makes it difficult to understand how they are protected in case of a problem.
- Competent authorities have limited powers to address consumer problems in their country as the authority of the country who issues the licence for a payment service provider (PSP) is responsible for supervision in all Member States.
- Consumers are often declared liable in case of theft due to a phishing attack or when their cards were stolen. This is due to the vagueness and lack of clarity of key definitions in PSD2 such as the definition of 'gross negligence' or 'fraudulent behavior'.
- Consumers struggle with a multitude of different authentication procedures as each payment service provider implements the much-needed strong customer authentication (SCA) differently and often does not guarantee that the authentication method can be used without owning the newest smartphone.

To ensure that payments are secure and convenient for consumers, the review of the Payment Service Directive 2 (PSD2) should fulfil the following objectives:

- The equivalent level of consumer protection applies no matter the statute of the payment service provider (PSP) and the category of payments.
- An efficient system of supervision (with a stronger role of the host Member State[1]) ensures sound enforcement of the Payment Service Directive and allows a smooth handling of consumer complaints.
- Consumers are protected against phishing attacks and fraudulent use of contactless cards by improved technical security measures, a fair liability regime and the possibility for consumers to easily identify the destination of each transaction.
- Strong customer authentication is easy to use thanks to a standardised authentication procedure, does not require a smartphone (or other sophisticated IT tools) to use it and is systematically applied for all transactions.

[1] PSD2 differentiated between home and host Member State, the home Member State being the one where the PSP is registered and the host Member State being the one where the payment service is offered.

1. Introduction

Payments have changed significantly for consumers since the entry into force of the Payment Service Directive 2 (PSD2): strong customer authentication replaced insecure procedures such as simply giving the number of the card (with CVV and date of issuance) or paper-based TAN (transaction authentication number) lists. FinTechs companies entered the payment sector and offer new services such as e-Wallets and alternative payment methods in e-Commerce. For consumers, this brings more payment method options and more competition can drive prices down. At the same time, this raises the question of the level of consumer protection: "Am I equally protected no matter the PSP I use?"

New actors also mean new supervisory challenges: Who needs to be supervised and by whom? Is a wallet provider just a technical service provider? Can a single competent authority effectively supervise several multinational companies such as Google, Amazon, Facebook, Apple and Alibaba?

Innovation also brings new security challenges and for consumers the difference between a secure payment transaction and a scam becomes blurrier: "Is it safe to enter my banking security credentials on a website of a third-party provider?" "Can I be sure that the payment goes to the right destination when I am scanning a certain QR-code?" "Is it safe to have a card in my pocket which allows me to pay €100 or even €250 without entering my PIN code?"

An important step towards more security was the introduction of strong customer authentication. But several hurdles remain to ensure that consumers can use this new procedure smoothly: "How do I use strong customer authentication for my online banking in the absence of the newest smartphone?" "Why is this authentication procedure so different from one provider to the other?" "How does strong customer authentication apply to instant payments in shops and peer-to-peer payments?"

This position paper discusses these questions and provides recommendations for the review of the PSD2 to make payments consumer-proof both in security and convenience. The position paper does not cover open banking as this should be addressed by the Open Finance Framework to ensure common rules.[2]

2. Scope

The PSD2 is characterised by a high level of complexity paired with legal uncertainty about which kind of service providers are covered by the Directive or excluded by numerous exemptions. A revised instrument should streamline the different statutes and reduce the number of payment services excluded from the scope.

2.1. Nature and architecture of the legal instrument

Several articles of the directive have been transposed differently across Member States as there were various regulatory options for its transposition (e.g. maximum liability amount in Article 74 on undetectable fraud) and divergences in implementation and interpretation (e.g. on scope exclusions, definition of gross negligence). In view of completing the internal market for payments and ensuring a harmonised transposition in all Member States with a

[2] BEUC's has already developed recommendations on Open Banking and Open Finance.

uniform protection for consumers - as they very regularly conclude cross-border payments - the Payment Service Directive 2 could become a Payment Services Regulation.

In addition, it should be logical to have all the payment legislation in a single text (following the recast principle). According to this logic, two existing pieces of legislation should be incorporated into the new PSD or PSR:

- The E-money Directive as modified by the MiCA Regulation (Market in Crypto Assets);
- The SEPA Regulation dealing with (instant and normal) credit transfers and direct debit.

2.2. Different statutes of payment service providers

The new instrument should be a single text gathering the various rules and statutes about payments.

There should be three different statutes of payment service providers (PSPs): payment institutions, credit institutions and e-Money institutions. Since Account Information Services do not provide payment services, they should be addressed in financial data space legislation.

- **Payment institutions** can provide all the services of Annex I but conversely to credit institutions and e-Money institutions, they cannot hold funds. As regards access to accounts, they just need to know if the funds are available on the payer's account.
- **Credit institutions** can provide all services of the PSD annex (e-Money issuance being added).
- **E-Money institutions** can provide e-Money services (incl. holding funds) and Payment institutions services.

The regulatory regime for payment institutions and electronic money institutions should be aligned where appropriate. For instance, consumers should be granted the same level of protection of their funds in case the e-Money institution goes bankrupt.

It should also be clarified that all institutions with direct consumer contact (i.e. a contract) are PSPs and have to hold a license as a payment, credit or e-money institution. For example, in the peer-to-peer domain or instant payment in shops there is an intermediary between the consumer and the bank. It is clearly a payment service which is proposed to the consumer. What is the legal statute for this provider? This point is unclear today. Is it a technical service provider or a PSP?

Another important question is whether Apple Pay and Google Pay are only technical service providers or payment service providers. Both companies consider these services as technical services which simply allow payment service providers to offer their payment services via mobile phones.[3] As these wallet providers operate at the front end (direct consumer contact), they have direct influence on how strong customer authentication is implemented, how information on different transactions is presented and the inaccessibility of the digital wallet could have an impact on the execution of the transaction. Therefore, wallet providers should be considered as payment service providers.

[3] Autorité de la concurrence française : Avis n° 21-A-05 du 29 avril 2021 portant sur le secteur des nouvelles technologies appliquées aux activités de paiement https://www.autoritedelaconcurrence.fr/sites/default/files/integral_texts/2021-04/21a05_0.pdf

2.3. The specific case of account information service providers

One of the main changes introduced by PSD2 has been the development of the category 'Account Information Service' (AIS). According to article 4.16 of PSD2, "account information service means an online service to provide consolidated information on one or more payment accounts held by the payment service user with another payment service provider or with more than one payment service provider". The statute of AIS has been used by many companies to access payment data (within the framework of open banking). According to PSD2, the access is given to payment accounts but not to the other accounts, such as saving accounts. Next to AIS, there are also Payment Initiation Service Providers (PISPs). But there is a major difference between these two categories of third-party payment service providers (TPPs): PISPs provide a payment service, which is not the case for AIS.

As the Commission has announced new legislation creating an EU data space for financial services, BEUC's recommendation is to remove the AISs from PSD2 to integrate them into the scope of this new legislation on open finance. For consumers, this would have a huge advantage as they would be protected by the same rules for access to their payment account, savings account, and other financial data. Otherwise, the rules will be different for various kinds of accounts which could be very confusing for consumers.

These operations are genuinely governed by the General Data Protection Regulation (GDPR), which created a contradiction with PSD2. As a result, the infrastructure (or more figuratively: the pipes) for extracting and processing sensitive data was created, whilst rules and oversight of data flows keep lacking behind. This jeopardises consumers' privacy. AIS shall fully comply with GDPR[4] and new legislation on open finance must create additional safeguards to prevent sensitive data from being shared at all i.e. a strict prohibition to use sensitive data without the possibility to overhaul the prohibition by consumer consent.

2.4. Scope exclusions

There are several scope exclusions which should be reconsidered as they left loopholes in the consumer protection of which consumers are often not even aware.

Telecom operators

Some telecom operators give the consumer the possibility to pay for some extra services through their mobile subscription bill. There are numerous complaints on payments by telephone bill (as reported by our members Altroconsumo,[5] OCU,[6] SOS Poprad, Stiftung Warentest,[7] vzbv[8]): consumers often only discover the real costs of the purchased services such as games, street parking, videos, magazines and all sorts of premium services once they receive their mobile subscription bill.
Using the phone bill to make a payment is a payment service and should be considered as such in PSD2. After strong lobbying by the telecom sector, this category of payment has been exempted from PSD1. Due to some abuse, the rules have been tightened by PSD2. Yet the new rules still exempt single payments of up to €50 and cumulative payments of up to €300/month from PSD2 which is clearly beyond the objective of exempting micro-payments (e.g. for a parking ticket).

---

4 For further reading, please see BEUC position paper on the interplay between GDPR and PSD2: https://www.beuc.eu/sites/default/files/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf

5 https://www.agcom.it/servizi-premium

6 https://www.ocu.org/tecnologia/internet-telefonia/consejos/servicios-pagos-a-terceros-telefonia

7 https://www.test.de/Handy-Abofallen-5505132-0/

8 https://www.vzbv.de/publikationen/schutz-vor-missbraeuchlichen-drittanbieterleistungen-im-mobilfunkmarkt

In addition, the text remains unclear on whether services from third-party providers where no contractual relationship between the telecommunication provider and the consumer exists, are also excluded from the scope of PSD2.This business model, where the telecommunication provider is just an intermediary, is widely used to offer all sorts of paid subscriptions and premium services to consumers under the guise of the telephone bill.[9] The Commission's interpretation[10] is that such intermediary services are not covered by the exemption.
In sum, the derogation for the electronic communication sector should be deleted to ensure that consumers are better protected against the miss-selling of additional services via telephone bills.

Independent ATM (automated teller machines) providers

BEUC recommends removing the exemption of ATM providers which are independent from banks or other PSPs. The aim of this exemption was to incentive the installation of stand-alone ATMs in remote and sparsely populated areas. Yet, according to the Commission, some PSP-operated ATM networks are considering the use of this exemption to redesign their business model and charge extra fees directly to the consumers, while terminating their current contracts with card schemes or card issuers. This is an unintended consequence of the PSD and justifies the removal of the ATM exemption. In addition, the EBA notes in its advice that the application of the exclusion is unclear, which also makes the supervision of ATM providers more difficult.[11]

Commercial agents

Certain intermediaries (e.g. fuel card issuing businesses) argue that they do not act as an intermediary but as merchants, based on the contractual arrangement (i.e. they purchase the good/service from the original merchant and sell it on to the consumer). Based on this arrangement, the intermediaries argue that they are exempted from the scope of PSD2. The exclusion for commercial agents should be re-assessed on that basis to cover such business models.

Limited networks

Examples of limited network payments are store cards, member cards, public transportation cards, petrol cards, restaurant vouchers or virtual wallets allowing for shopping on specific websites. The current PSD provision exempts payment activities which take place in the context of a limited network without however defining, for instance, the notion of what is a 'limited' network and what is a 'limited range of products/services'. As a result, activities covered by this exception often comprise a high number of shops, massive payment volumes and hundreds or thousands of different products and services, which has nothing to do with the original limited network concept. This implies uncertainties for market actors and greater risks for consumers. The exemption on 'limited networks' is still unclear, and the exemption of payment instruments used within huge limited networks is inappropriate (as also reflected by the EBA in its advice on the definition of limited networks). BEUC thus recommends adding a clear definition of limited networks in a revised PSD2 which restricts this exemption to a small number of shops.

9 https://www.test.de/Handy-Abofallen-5505132-0/
10 https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4181
11 https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2022/Opinion%20od%20PSD2%20review%20%28EBA-Op-2022-06%29/1036016/EBA%27s%20response%20to%20the%20Call%20for%20advice%20on%20the%20review%20of%20PSD2.pdf

3. Supervision

Competent authorities have a key role in ensuring that consumers can safely issue and receive a payment without losing their money or their personal data. The current system is not effective for law enforcement and leaves consumers in the dark when a dispute arises: it is difficult to launch a complaint to the competent authority, let alone to be compensated for the harm suffered.

The problem

The European passporting regime allows payment institutions to search for authorisation in one Member State and then provide their service across all Member States. This system brings the risk of forum shopping meaning that providers may eventually seek authorisation in those Member States that have the most liberal authorisation regimes or that are simply too small in terms of resources to cope with the supervision of companies operating across the Union.

It seems that some countries are more attractive than others for payment institutions. Ireland, Luxembourg and Lithuania are supervising the largest BigTech and FinTech companies:

- Luxembourg: Amazon, Alipay, and Wordline, Paypal (as a credit institution);
- Ireland: Facebook, Google (as a payment institution), Apple (service provider excluded from the scope of PSD2);
- Lithuania: Google (as an electronic money institution), Revolut.

This means that the competent authorities of these three countries are responsible for ensuring compliance with PSD2 for those companies (and many others) in all Member States and the countries of the European Economic Area. The so-called home Member State (where the payment institution is registered) can cooperate with the host Member State (where the service is provided). But the host Member State depends on the home Member State to take action if problems arise within its territory.

For consumers, the passporting regime brings an additional hurdle in case they want to notify a problem to the competent authority. Consumers naturally believe that they can address the competent authority of their home country as they are not aware of the passporting regime. But they will then be referred to the competent authority of the home Member State of the payment institution which often does not speak their language, is less familiar with the national specificities of the host Member State and might have less of an incentive to address issues in another Member State than the host competent authority would have.

The solution: the driving-license approach

Supervision of the ongoing activities of payment institutions should be performed by the competent authorities of the host Member State as they are better situated to perform this task (e.g. on-site inspections): capacity to process information in the national language, knowledge of the national market and cooperation with other national competent authorities (e.g. consumer protection authority, data protection authority).

BEUC recommends following the concept of the European driving licence: you pass the test to acquire a European driving licence in one country which enables you to drive in all EU Member States. But if you do not respect the road traffic regulations, the Member State where you drive, will be able to take all necessary measures (including revoking the driving licence) in case of breaches of their traffic regulation.

Translated to payment services, a payment institution gets authorised in one Member State (home Member State) and the host Member State will have day-to-day supervisory powers and enabled to take all necessary measures in case of breaches with payment legislation. This shall include the possibility to revoke the European passport of the payment institution which is essential to prevent further failure in up to 26 other Member State markets. To ensure consistent sanctioning across the EU, the driving licence approach should be complemented by a rulebook foreseeing a minimum level of fines to be imposed in case of non-compliance with PSD.

In addition, the European Banking Authority (EBA) could become a central coordinating authority for cross-border-complaints by discussing with the relevant authorities cross-border consumer protection concerns. With multinational companies entering the payment sector, monitoring makes more sense at a European level. This will allow authorities to coordinate action in case of breaches of the rules. To give one example, TikTok so far is not licensed as an e-money institution despite offering e-money services: TikTok offers consumers the possibility to buy e-money (so called "coins") and send them in the form of virtual gifts to their favourite content providers. The content provider can then exchange the virtual gifts back to a fiat currency. TikTok determines the value of the virtual gifts without a transparent exchange rate and withholding around 50% of the initial sum according to the BBC.[12] To maintain this business model, TikTok refuses to get a licence as an e-money institution. So far, none of the national competent authorities has taken action.

Finally, it should be easier for consumers to find out which authority is competent for a certain payment service provider (Article 52, paragraph 1b) or payment initiation service provider (Article 45, paragraph 2b) and the relevant contact details. Consumers could receive this information for instance via a QR code giving them direct access to the relevant contact details.

4. Security and liability

Despite strong customer authentication, fraud continues to exist and can cost consumers thousands of euros. 60% of the 4,300 complaints received by our French member UFC Que Choisir between 2019 and 2022 were above €4,000. In all these cases, the bank refused to refund the amount to the consumer.[13] BEUC's Greek member EKPIZO has received 600 complaints in 2022 alone about online banking fraud with losses ranging from €40,000-50,000. According to the Bank of Greece, in 2021 there were 8,635 registered cases of online fraud involving €26m.[14]
This chapter looks at different types of fraud cases, the current security and liability regime and possible solutions ensuring that consumers get refunded in case of fraud.

4.1. Social engineering (phishing)

The problem

Banks try to give consumers various tips and tricks on how to avoid phishing attacks – the problem is that phishing techniques are evolving fast and tricks to avoid falling into the hands of a fraudster may not help consumers in more sophisticated cases or even worse, may increase the consumer's confidence in their capacity to identify phishing attacks.

12 https://www.bbc.com/news/technology-48725515
13 https://www.quechoisir.org/action-ufc-que-choisir-refus-de-remboursement-des-fraudes-bancaires-l-ufc-que-choisir-depose-plainte-contre-12-banques-n101896/
14 https://balkaninsight.com/2022/10/31/in-greece-e-banking-fraud-is-on-the-rise-and-consumers-are-vulnerable/

Trick No 1: Check the contact details

Consumers are told that they can identify a fraudster by unknown phone numbers and should be especially vigilant when they are called by foreign numbers. But fraudsters can call consumers with a phone number from the bank or appropriate themselves the phone number of the consumer's personal contacts (so-called 'spoofing').

Our Dutch member Consumentenbond warns against fraud via WhatsApp[15]: fraudsters will install WhatsApp on their phone and try to connect to the consumer's account with consumer's phone number. In a second step, the fraudster will use the consumer's WhatsApp to contact friends and family of the consumer to ask for money. For friends and family, based on the contact details, it will be impossible to identify the fraud and it is likely that they trust the fraudster and transfer them some money.

Our UK member Which? reported a case where a consumer was called by a telephone number from Barclays with the fraudster having access to the consumer's account details. Based on the fact that the phone number was trustworthy and the fraudster had all this insider knowledge, the consumer trusted the fraudster. The fraudster pretended to be part of Barclays' fraud team and to secure the money in their account, the consumer had to transfer money to another account. Under pressure, the consumer transferred €12,000. The consumer got reimbursed only after several months and the involvement of Which? in this fraud case.[16] UFC Que Choisir reports similar cases which ended even worse for consumers as the bank refused to pay due to assumed "gross negligence".[17]

Trick No 2: Do not share your passwords

Do not click on links or attachments in e-mails, do not enter your bank account details on websites which you do not know. In times of open banking and new technologies, following instructions like this is easier said than done.

Our German member vzbv did a study on how account information services implemented the authentication requirements of PSD2.[18] In only three of the 15 cases, consumers were redirected to the website of their bank. In 11 cases, consumers had to enter their bank credentials directly on the website of the account information service. The confirmation of the second factor was designed in very different ways, in one case a TAN had to be confirmed three times. The German Federal Security Agency is warning consumers at the same time to be vigilant when several TAN have to be entered in a row.[19] For consumers it becomes very difficult to distinguish between a 'serious' service provider and a fraud case.

Our Belgian member Test-Achats reported cases where fraudsters gained access to the consumer's bank account by QR code.[20] The consumer sells an object via an online marketplace and is contacted by a potential buyer. The buyer tells the consumer that they will transfer the money to via their professional bank account and asks for the IBAN. To confirm the IBAN, they send the consumer a QR code to scan which is done via the mobile bank app of the consumer. The problem is that the QR code is not a confirmation of payment but hides a link towards a connection portal which gives the fraudster direct access to the consumer's bank account.

---

15 https://www.consumentenbond.nl/veilig-internetten/whatsapp-fraude

16 https://www.which.co.uk/news/article/ive-been-stonewalled-by-barclays-months-after-losing-12k-to-a-scam-how-can-i-get-my-money-back-auDTu1S0qoMz

17 https://www.quechoisir.org/actualite-arnaque-des-banquiers-tres-bien-imites-n98399/

18 https://www.vzbv.de/sites/default/files/2022-06/2022-06-14%20KID_Ergebnispapier-final.pdf

19 https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Online-Banking-Online-Shopping-und-mobil-bezahlen/Online-Banking/Was-tun-im-Ernstfall/was-tun-im-ernstfall_node.html

20 https://www.test-achats.be/hightech/internet/dossier/phishing

The current liability regime

The fundamental concept of liability is that the party with most control over the system should bear the most liability. This means that banks have the responsibility to become more cybersecure and to identify fraud proactively and if they fail to do so, they need to compensate consumers for the money lost. If this principle applies, banks will invest more to prevent being held liable, this will be less costly and more sustainable than ex-post damage compensation.

The current liability regime and how it is currently enforced, falls short on this fundamental principle.
There are two possible scenarios: an authorised and or an unauthorised transaction. In the case of an authorised transaction, the consumer is liable for the full amount.

In the case of an unauthorised transaction, the bank must refund the consumer (Article 73, PSD2). There are however two exceptions (Article 74, PSD2):

- The consumer is liable up to a maximum of €50 where the unauthorised payment transaction results from the loss or, theft or misappropriation of a payment instrument which was detectable to the payer prior the payment or where the loss was caused by the bank.
- The consumer is liable for the full amount if the consumer acted fraudulently or with gross negligence.

As reported by our members (Arbeiterkammer[21], vzbv[22], Norwegian Consumer Council[23], Which?[24], UFC Que Choisir[25], Consumentenbond[26]), banks refuse to reimburse the consumer and claim that consumers are liable as they have authorised the transaction e.g. by entering their security credentials or by claiming that the consumer has acted with gross negligence. In France, banks systematically refuse to refund the consumer when strong customer authentication was used. In Germany, being victim of a phishing attack is considered as gross negligence in most cases of current case law.

As a result, consumers must bear losses of several thousands of euros, in some cases their whole savings for the education of their children or their pension.

The solution

The PSD2 review should look both at technical and legal solutions to better protect consumers when they become victims of fraud attacks.

In terms of technical solutions, the following questions should be assessed:

- What additional obligatory measures on the side of payment service providers (like AI-based transaction monitoring mechanisms) could prevent social engineering attacks more effectively?

21 https://stmk.arbeiterkammer.at/beratung/konsumentenschutz/internet/Phishing__AK_holt_Geld_bei_Banken_zurueck.html, https://www.arbeiterkammer.at/beratung/konsument/AchtungFalle/Phishing-E-Mails_von_Banken.html

22 https://www.vzbv.de/sites/default/files/2022-07/220720_PSD2_vzbv.pdf

23 https://www.forbrukerradet.no/siste-nytt/bankene-ignorerer-lovverket-svindelofrene-taper/

24 https://www.which.co.uk/news/article/which-calls-on-banks-to-come-clean-about-fraud-refunds-ar4J67l2GAsz

25 https://www.quechoisir.org/action-ufc-que-choisir-refus-de-remboursement-des-fraudes-bancaires-l-ufc-que-choisir-depose-plainte-contre-12-banques-n101896/

26 https://www.consumentenbond.nl/acties/vergoed-bank-oplichting

- How can payment service providers and third-party providers clearly identify themselves towards consumers? Can mandatory redirection to the bank interface make authentication safer?
- Can an IBAN check and a request to pay system reduce fraud cases linked to a mismatch between the name and the IBAN of the payee?

In terms of legal solutions, to reduce legal uncertainty, the liability regime must be complemented by clearer definitions of 'gross negligence', 'reasonable grounds to suspecting fraud', 'fraudulent act' as suggested by the European Banking Authority.[27] Otherwise it will be left to PSPs to define in their terms and conditions what 'gross negligence' and 'fraudulent act' means. The term 'authorised transaction' should be re-assessed in the light of new technological developments: for consumers it is not always clear for which purpose a QR-code or TAN is used: to log in, to cancel or to authorise a transaction?

In addition, for authorised transactions, there needs to be a new liability framework. Social engineering is specifically targeting the vulnerabilities of consumers rather than technical weaknesses. Therefore, fraud based on authorised transactions is becoming more frequent. The Commission should review the liability regime ensuring that consumers are not held liable when being tricked into authorising a transaction. Inspiration could be gained from the current discussions in the UK on the Financial Services and Markets Bill. Under these proposals announced in September 2022, banks will be forced to reimburse anyone who loses more than £100 to bank transfer or payment fraud, apart from exceptional circumstances. This should mean most victims are fully reimbursed – putting an end to the reimbursement lottery they face. The proposal foresees that any fraud victims deemed to be vulnerable should be reimbursed without exception.[28]

Moreover, it should be clarified that the burden of proof is on the PSP when the refund is called into question. It should also be clarified that *prima facie* as a means of proof is insufficient. According to PSD2, PSPs must refund the payer immediately, on the following working day at the latest. Exemptions only apply in the case of suspicion of fraud that banks report to the national authority in writing. However, in practice, PSPs regularly shift the blame on consumers and, without proof, allege gross negligence on the payers' side. This puts consumers at a huge disadvantage. When a consumer's account has been cleared out by fraudsters and the PSP acts as described, the consumer faces significant legal fees and an administrative and emotional burden to resolve the banks' allegations. The review of PSD2 should clarify that PSPs have to refund payers immediately irrespective of disputed allegations. PSPs can then in a second step introduce a claim for compensation in case gross negligence can be proved.

Finally, supervisory authorities should get a better data overview of whether consumers are reimbursed in case of fraud and if they are not reimbursed for which reason. In this regard, the European Banking Authority recommends turning their guidelines on fraud reporting into regulatory technical standards.[29]

---

27 https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2022/Opinion%20od%20PSD2%20review%20%28EBA-Op-2022-06%29/1036016/EBA%27s%20response%20to%20the%20Call%20for%20advice%20on%20the%20review%20of%20PSD2.pdf

28 https://press.which.co.uk/whichpressreleases/people-experiencing-mental-health-problems-twice-as-likely-to-fall-into-debt-due-to-fraud-which-finds/

29 https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2022/Opinion%20od%20PSD2%20review%20%28EBA-Op-2022-06%29/1036016/EBA%27s%20response%20to%20the%20Call%20for%20advice%20on%20the%20review%20of%20PSD2.pdf

4.2. Contactless cards

For contactless cards, similarly to cash, the risk is that in case the card is lost or stolen, the thief can use the card without being asked for a PIN code up to a certain amount. This section will look at the security mechanisms and the liability regime.

Security mechanisms

Card schemes and the banking sector increased the thresholds for contactless payments during the COVID-19 pandemic. Consumers only need to enter their PIN code when they pay more than €50, compared to €25 or €30 previously. Although BEUC does not oppose the measure, we insist that the raising of these thresholds to €50 should be completed with the freedom of choice. A consumer should be able to ask their bank to have a card without the contactless functionality and should also be able to choose the maximum amount for which they can use the contactless card within the legal threshold of €50.

Commercial credit cards have asked the European Banking Authority to increase the amount of no-PIN contactless payments to €250. For BEUC, any potential increase is unacceptable. Having a contactless card will be the same as having €250 in cash in your pocket. With the difference that you can easily adapt the amount of cash you take with you. The €250 on the contactless card will always be in the consumer's pocket, also in a full metro, or at a party for example. Once again, it is an incentive to fraud. In addition, making payments more convenient also facilitates overspending and consumers can lose control over payments.

According to the regulatory technical standards for strong customer authentication (Regulation 2018/389) (Article 11, point b and c), PSPs must choose which other security limit they put in place:

- A PIN code requested after five transactions, or;
- A PIN code requested if the cumulative amount of the last transactions is above €150.

BEUC considers that the two security limits should apply at the same time, not only one.

Consumers increasingly use e-Wallets (e.g. Apple Pay, Google Pay) to pay with their phone (via near-field communication). There are different approaches in terms of security, while some providers require the consumer to unlock their phone to pay contactless, other providers also allow payment with a blocked phone. To ensure secure payments, it should be required to unblock the phone to make a payment.

Liability regime

A consumer can contest any contactless transaction (Art 74 PSD2), but the procedure is complicated and can be a hassle. The situation has been worsened since the Deniz-bank judgement[30] by the Court of Justice of the European Union (CJEU) as the judgement increased legal uncertainty, as explained below.

If a contactless card is used fraudulently, three possible articles of PSD2 could apply to determine the amount for which the consumer is liable:

- Article 74, paragraph 1, first subparagraph: as a general rule when a card is stolen and used, the liability of the consumer is limited to €50 for transactions before the notification of the loss.

[30] https://curia.europa.eu/juris/liste.jsf?num=C-287/19

- Article 74, paragraph 2 could apply if a contactless card is used without SCA: the consumer is not liable and will be reimbursed of the full amount. It was the position of the European Commission as stated in the Retail Payment Strategy.[31] But since then, the Court of Justice of the European Union has published the Deniz-bank judgement coming to a different conclusion.
- Article 63, paragraph 1 applies to anonymous transactions. In that case according to PSD2 the liability of the consumer is limited to €30 for a single transaction and €150 for multiple transactions. The judgment of the CJEU concludes that contactless transactions are anonymous transactions and therefore Article 63 applies.[32]

After the Court judgement on contactless cards, there are a lot of doubts on the interpretation: From our viewpoint, the CJEU erred in categorising the technology when concluding that contactless cards fall under article 63 because near-field-communication is a communication technique not a payment instrument. In addition, it is not explicitly mentioned in the Court judgement that the consumer is no longer protected by article 74, paragraph 2 in the absence of SCA. BEUC recommends clarifying when PSD2 is revised, that article 74, paragraph 2 applies as a liability regime for contactless cards.

4.3. Unconditional right to refund for direct debits

This unconditional right should be maintained as it stands. First of all, there was no abuse from consumers of this right. Instead, it has been very useful in practice: e.g. at the beginning of the COVID pandemic, many sport clubs etc. continued to collect payments without providing a service.

5. Further improvements to strong customer authentication

BEUC fully supports strong customer authentication (SCA) as a means to reduce fraud. As explained in the chapter on security and liability, the financial damage can be huge where security measures are insufficient to protect consumers' bank accounts. While SCA has been a successful measure in general, several further improvements are necessary to increase security while ensuring inclusive application.

5.1. Inclusive strong customer authentication

A significant number of consumers do not want to use smartphones for online banking. This can be for several reasons: a) Consumers do not own a smartphone; b) they cannot operate a smartphone; c) their smartphone does not operate the required app (often because operating systems are only updated for a short period by producers); d) for security concerns or; e) for concerns over their privacy.

Unfortunately, the PSD2 does not address this widely held consumer concern. In practice, consumers have to improvise. If the bank offers alternative authentication methods, they have to buy dedicated devices (e.g. chipTAN) which are not always compatible with other banks or might be abolished as an authentication method at a later point in time.

The PSD2 review should look at solutions which allow consumers to use an authentication method which is:

- Not exclusively smartphone-based (e.g. via chipTAN);

[31] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0592&from=EN
[32] https://curia.europa.eu/juris/liste.jsf?num=C-287/19

- Available at no additional cost;
- Allowing consumers to switch bank and maintain the authentication device;
- Considering the needs of vulnerable consumers.

5.2. A standardised authentication procedure

Consumers struggle with multiple authentication procedures: it makes it more difficult to identify phishing attacks (see chapter 3), it deteriorates the possibilities to use multi-banking (e.g. administering several different bank accounts in one app) and it makes online banking more difficult for consumers with a lower level of digital skills.

The only secure authentication solution is redirection to the home bank where the consumer then enters directly their security credentials. In other words, where no personal credentials are shared with any third-party provider. This should be embedded in a standardised procedure e.g. no multiple requests to enter TANs etc.

5.3. Rules for transactions where the amount is not known in advance

PSD2 Article 75 foresees the possibility of introducing maximum limits for the amounts to be blocked on the payer's payment account when the exact transaction amount is not known in advance. It was questioned whether SCA needs to be repeated in case the amount is above the maximum limit.

There is no need to modify this article. With regards to the above, for card-based payment transactions where the exact transaction amount is not known in advance, if the final amount is higher than the amount the payer was made aware of and agreed to when initiating the transaction, the payer's PSP shall apply SCA to the final amount of the transaction or decline the transaction. If the final amount is equal to or lower than the amount agreed in accordance with Article 75(1) of PSD2, the transaction can be executed and there is no need to re-apply SCA, as the authentication code would still be valid in accordance with Article 5(3)(a) of the Delegated Regulation. This applies also to card-based payment transactions where the exact amount is not known in advance and funds are not blocked by the payer's PSP in accordance with Article 75(1) of PSD2. This is in line with the reply given by EBA to the question on how to interpret this article.[33]

5.4. Low value transactions

Article 16 of the regulatory technical standard 2018/389 is dealing with low value transactions. It states that the SCA is not needed when the transaction is below €30. This exemption is another entry point for fraud: it allows a fraudster to purchase goods/services online with a stolen card. BEUC recommends that the first transaction to a new beneficiary, even for one euro should request SCA to prevent fraud. The derogation for low value transactions should be valid only after the first transaction with the same payee.

5.5. Payment in shops/peer-to-peer

Payments via QR-code (i.e. instant or non-instant credit transfers) in shops or peer-to-peer are so far considered to be a remote payment transaction. Conversely to a card payment in shops, for this kind of payment, strong customer authentication requires dynamic linking meaning that it requires linking of the transaction to the specific amount and the specific payee (Article 97, paragraph 2, PSD2). This renders these payments complicated in practice.

[33] https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5133

To facilitate these payments in the future, the definition of proximity payments needs to change which is currently limited to transactions not initiated via the internet. Payments by QR-code are using a dedicated app on the mobile device of the payer which is using the mobile internet. However, the relevant factor here should be that, similar to a card payment, the payer and payee are physically present when initiating the payment which reduces the risk of tampering and therefore no dynamic linking should be required.

6. Other topics

6.1. The surcharge ban on card-based payment methods

Article 62, paragraph 4 foresees a surcharge ban for card-based payment methods which are subject to the Interchange Fee Regulation. BEUC has been supportive of this ban as it ruled out excessive surcharges which were until PSD2 entered into force particularly common in the airline sector.[34] For consumers, this meant that the price to be paid was higher than the one initially advertised for.

6.2. Identification of a transaction

The clarity of information about the past transactions is a basic and crucial element in combatting fraud. Experience has shown that in many cases the consumer had a lot of difficulties to identify the transaction. For this reason, a working group of the European Retail Payment Board (ERPB) has been created. ERPB has concluded that the consumer should be aware of with whom, where and when the transaction has been executed. To allow consumers to easily identify a transaction, this information should include the commercial trade name and not only the legal name of the companyConversely, in several Member States, existing legislation obliges PSPs to provide the legal name of the company which often has no connection with the trading name. Article 57 is dealing with "information for the payer on individual payment transactions". By point 57(a), it is stated that the consumer should receive "a reference enabling the payer to identify each paymenttransaction". Therefore, BEUC proposes to reinforce the Alinea 57(a) by adding that the commercial trade name of the payee should be provided to the consumer.

END

[34] https://www.beuc.eu/press-releases/end-card-surcharges-days-away

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EISMEA. Neither the European Union nor the granting authority can be held responsible for them.