The Consumer Voice in Europe

PAYMENT SERVICES

BEUC's recommendations on the Payment Services Regulation and the Payment Services Directive 3

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-2023-123 - 29/09/2023

Why it matters to consumers

Payments are part of our everyday life when purchasing goods and services. However, the way consumers pay is changing. Payment options have multiplied: while coins, banknotes and cards remain important, payments increasingly take place online and via mobile phones. This allows for more convenience but also brings new challenges to keep consumers' bank accounts, payment cards and e-wallets secure.

Summary

The following table summarises the Commission proposal and BEUC's position on the different elements. Where BEUC considers that the approach taken by the Commission is not beneficial to consumers, recommendations to improve the text are provided in the paper itself.

The table assesses the proposals with the following symbols, illustrating whether BEUC:

 *rejects the proposal*

 *supports in principle but there is room for improvement*

 *supports the Commission proposal*

 *considers that an important point is missing*

Commission proposal	BEUC position
 **Scope:** The Regulation now covers both payment and e-Money services in one text. Scope exemptions are largely kept for limited networks, electronic communication providers and technical service providers. Limited networks will be further defined by the European Banking Authority. The exemption for independent ATMs has been removed.	 BEUC supports the integration of e-Money services into the payment services regulation as it will ensure that consumers are equally protected. BEUC welcomes that independent ATMs are now included in the scope but regrets that a wide list of exemptions remains and that e-wallets (e.g. Apple/Google Pay) stay unregulated.
 **Transparency**: Payment service providers (PSPs) must now indicate the time a credit transfer or money remittance will take to a payee outside the EU. Charges must be expressed as a mark-up on the exchange rate referenced by the central bank. ATMs must indicate all charges for cash withdrawals prior to the withdrawal. Payment transactions must indicate the commercial trade name of the payee.	 BEUC supports the new transparency requirements which will allow consumers to compare different offers in terms of price and speed when sending money for example to their family living in a third country. The same goes for cash withdrawals, consumers are now warned about the costs of an ATM. Indicating the commercial trade name will allow consumers to easily identify whom they paid and check if no mistake has been made.

Accessibility: PSPs must provide a **S**trong **C**ustomer **A**uthentication method which can be used without owning a smartphone and merchants can now offer withdrawal of cash without purchase up to €50.	BEUC supports these additional rules contributing to financial & digital inclusion. A smartphone independent authentication should be available at no additional cost. As regards withdrawal of cash in shops, a higher threshold would be welcome.
Funds blocked for example for a car rental or hotel accommodation have to be proportionate and must be released immediately once the exact amount of the good/service is known.	BEUC supports the new rules to speed up the release of blocked funds and prevent unreasonably high amounts being blocked.
Open banking: Consumers receive a dashboard in their online banking where they can grant and withdraw access to third parties and receive an overview for which purpose data has been shared. Banks have stricter criteria to follow based on which they can refuse third party access.	BEUC supports open banking in view of more competition, but this cannot come at the expense of data security. Consumers should not be asked to enter personal security credentials on third party websites. Personally-sensitive data must be well-protected and consumers should receive a guarantee that they are not refused access to a product or service when refusing to share their data via open banking.
Fraud prevention: PSPs must provide an IBAN name check indicating whether there is a discrepancy between the name of the beneficiary and the IBAN. PSPs have to monitor transactions and can share information on fraudulent IBANs with other providers.	BEUC supports the introduction of an IBAN name check for all credit transfers and the obligation to monitor transactions. The information sharing of fraudulent IBANs should become mandatory for PSPs to mitigate further fraud cases.
Liability regime: PSPs are now liable for authorised payment fraud where the name of the bank has been used to trick the consumer into the transfer. PSPs are also liable if they fail to identify a discrepancy in the IBAN check.	Despite several positive changes, consumers will remain liable in most cases of phishing and spoofing. In addition, it remains unclear who has to prove "gross negligence" and PSPs will likely continue holding consumers liable for the fraud.
Enforcement: Competent authorities receive investigatory powers and more specific rules on administrative sanctions are introduced. The EBA receives product intervention powers in the field of payments.	BEUC supports more structural enforcement but in addition to sanctions, remedies should be foreseen for consumers. In addition, PSPs should be obliged to participate in alternative dispute resolution and accept its outcome.
Supervision: The supervisory regime remains unchanged with the competent authority of the country where the PSP registered being fully responsible for supervising it.	The current system is not effective for law enforcement as in cross-border situations, the host country authority cannot take action and consumers cannot file a complaint about a PSP in their Member State when the PSP is registered elsewhere.

1. Introduction

Consumers want payments to be secure, to ensure neither their money nor their data is lost in the process.

This means that consumers are protected no matter how they pay, with their card, via their banking app, or via an e-wallet. Currently e-wallets are not regulated while becoming a key user interface for payments.

Open Banking can offer consumers interesting services such as new payment providers or tools to manage their budget, but consumers should remain in full control of their data and should not be refused a good or service when they decide not to share their data.

Phishing, spoofing, fake bills or fake shops – there is a long list of payment fraud scenarios and in most cases, consumers are held liable for the financial loss. In the future, there should be more systematic reimbursement for fraud victims.

When fraud happens, there should be easy ways for consumers to seek redress. Alternative dispute resolution is one of them but often payment service providers refuse to participate in the schemes. Therefore, mandatory participation should be considered.

To achieve better structural enforcement, for example of the liability regime on fraud, competent authorities should be able 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.

The following chapters will summarise BEUC's recommendations for the Payment Services Regulation and the Payment Services Directive 3. Where BEUC is satisfied with the Commission text, this is indicated in the summary table but not replicated in the following chapters.

2. Scope of the proposal

While the Regulation adds clarity by covering all payment services providers in a Regulation, a wide list of exemptions remains.

Particularly detrimental is the exemption for telecommunication providers who charge consumers via their mobile subscription bill. There are numerous complaints on payments by telephone bill as reported by our members Altroconsumo, OCU, SOS Poprad, Stiftung Warentest, vzbv)[1]. 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.

In addition, exemptions for providers of meal vouchers remain in the PSR without a particular reason. In the case of meal vouchers, this allows operators of such schemes to charge merchants high fees which, as a consequence, limits the acceptance of meal vouchers and hence the possibility for consumers to spend their employment benefits.

[1] Various articles from BEUC members on subscription traps with telecom providers: https://www.agcom.it/servizi-premium, https://www.ocu.org/tecnologia/internet-telefonia/consejos/servicios-pagos-a-terceros-telefonia, https://www.test.de/Handy-Abofallen-5505132-0/, https://www.vzbv.de/publikationen/schutz-vor-missbraeuchlichen-drittanbieterleistungen-im-mobilfunkmarkt

The Regulation should also be made future-proof by adequately considering the role of e-wallet providers such as Apple Pay, Google Pay and Samsung Pay. E-Wallet providers are currently considered as technical service providers and hence out of scope of the Payment Services Regulation. But, conversely to other technical services working in the back end, e-Wallets have now become the key interface through which consumers manage their online banking. Technical service providers manage payment transaction data, support strong customer authentication and, in the future, the IBAN name check during the payment transaction, decide how information on charges and fees is passed on to consumers. But technical service providers are not in the scope of the Payment Services Regulation with the exemption of being liable if they fail to support strong customer authentication. This means that technical service providers do not have any obligations on how to provide information to consumers (e.g. information on charges for money remittances). As a consequence of being out of the scope of the Payment Services Regulation, they are also not subject to the Digital Operational Resilience Act (DORA) which lays down uniform requirements for financial operators on how to manage security incidents of network and information systems. E-Wallets should be treated in a similar way to account information service providers, for instance when it comes to digital operational resilience in accordance with DORA.

3. Open Banking

BEUC supports open banking in view of more competition, but this cannot come at the expense of data security. The Payment Services Regulation must keep consumers' data secure; this includes security credentials and data included in the payment transactions.

First and foremost, consumers should not be discriminated against or refused access to a service or product (e.g. credit) when they refuse to use open banking as a means to provide data. They should be offered different ways to provide the data required to access the service (e.g. credit) or different ways to initiate a payment.

BEUC considers that the term "permission" should be clarified to avoid any ambiguity related to the legal bases necessary for processing personal data under the GDPR. In this sense, the term "permission" should not to be understood as "consent", "explicit consent" or "necessity for the performance of a contract" as per the GDPR, in line with the EDPS Opinion.

When consumers consent to share data with third parties, data sharing should not become an "open bar,"[2] but there must be strict enforcement of the principles of data minimisation and purpose limitation. Only data which are strictly needed for the performance of a contract, shall be accessed (Art. 5(1) c GDPR). The European Data Protection Supervisor should be mandated in the PSR to issue guidance on how to implement the obligations of GDPR for open banking. For services where personally sensitive data is not needed, processing of such data shall be prohibited as foreseen in Article 18 of the Consumer Credit Directive for creditworthiness assessments.

[2] For more information, please read BEUC (2020): Making Open Finance consumer friendly. Available here: https://www.beuc.eu/sites/default/files/publications/beuc-x-2020-054_making_open_finance_consumer-friendly.pdf

BEUC also rejects the extension of Article 80 PSR which now gives payment systems the possibility to process special category data (Article 9 GDPR) and allow processing of such data whenever necessary for the "public interest or the well-functioning of the internal market for payment services". Previously, such processing was only foreseen for fraud prevention and it is not clear why such a wide extension was proposed in the PSR. Using special categories of data for the suggested purposes is at odds with data protection by design and by default.

Given the sensitive nature of payment transaction data revealing a lot about a consumer's private life, consumers shall be adequately informed when this data is used to create a personalised offer and which categories of data have been used to create such an offer. Where automated decision-making is used, similarly to Article 18 of the Consumer Credit Directive, consumers must be informed and should have the right to human interaction.

In addition, it shall be explicitly foreseen that consumers cannot be discriminated against on the basis of any other types of personal characteristics such as gender, disabilities, nationality or place of residence similarly to Article 6 of the Consumer Credit Directive.

To avoid that consumers' personalised security credentials are shared with any third party, account information service providers and payment initiation providers should always redirect consumers to the website of their online banking to authenticate themselves. BEUC thus rejects the Commission proposal to consider re-direction as an obstacle to open banking and would rather see it as the preferred and only option to access data.

BEUC supports the introduction of dashboards to grant and withdraw access for third party providers including data perimeters indicating the categories of data which are processed. It should however, be clarified that when withdrawing access or when the period of validity of the permission ends, TPPs must also erase all data accessed previously. There is a risk that some consumers have not understood what they have agreed to. Consumers should thus be able to determine *ex ante* that they will never give a right to third parties to access their bank account.

Moreover, information on data categories to consumers must be easy to understand. The lists of data categories should be standardised via a regulatory technical standard. Otherwise, operators are likely to use vague formulations to describe the categories of data and fail to provide clear and understandable information to consumers. Consumers should also receive the information when data has been retrieved.

In addition, BEUC questions how the data holder (the consumer's bank) can control the security of processing (Article 32 GDPR) and how data minimisation is implemented if the consumers' bank is not allowed to verify whether the consumer has given permission to data access by a third-party provider. In addition, financial supervisors shall cooperate with data protection authorities to enforce GDPR and PSR rules in open banking.

In more general terms, rules on the protection of personal data should remain aligned with the framework of Open Finance. Rules on administrative sanctions should be aligned while maintaining the most stringent set of rules.

vzbv study: Difference between professional providers and fraudsters becomes blurry

When using open banking, consumers are often asked to enter their bank credentials on third-party websites and to enter multiple TANs in a row, as **vzbv** discovered. At the same time, fake websites are getting more professional and harder to identify. The risk is that consumers "learn" that it is acceptable to enter their online banking credentials on third party websites and can more easily fall into the trap of fraudsters using the same methods to get access to consumers' online banking.
Read more: https://www.vzbv.de/sites/default/files/2022-06/2022-06-14%20KID_Ergebnispapier-final.pdf

4. Fraud

Currently, consumers bear 68% of the losses according to EBA data[3]: consumers are not reimbursed when they supposedly authorised the payment or when they acted with "gross negligence". Despite several changes, consumers will remain liable in most cases of social engineering fraud such as phishing and spoofing. BEUC welcomes that in case of bank impersonation fraud, consumers shall get reimbursed, but this leaves out a wide range of payment fraud cases where consumers will also be held liable in the future. For instance, the provision remains weak in comparison to recently adopted rules in the UK[4] foreseeing consumer reimbursement for all authorised push payment fraud[5].

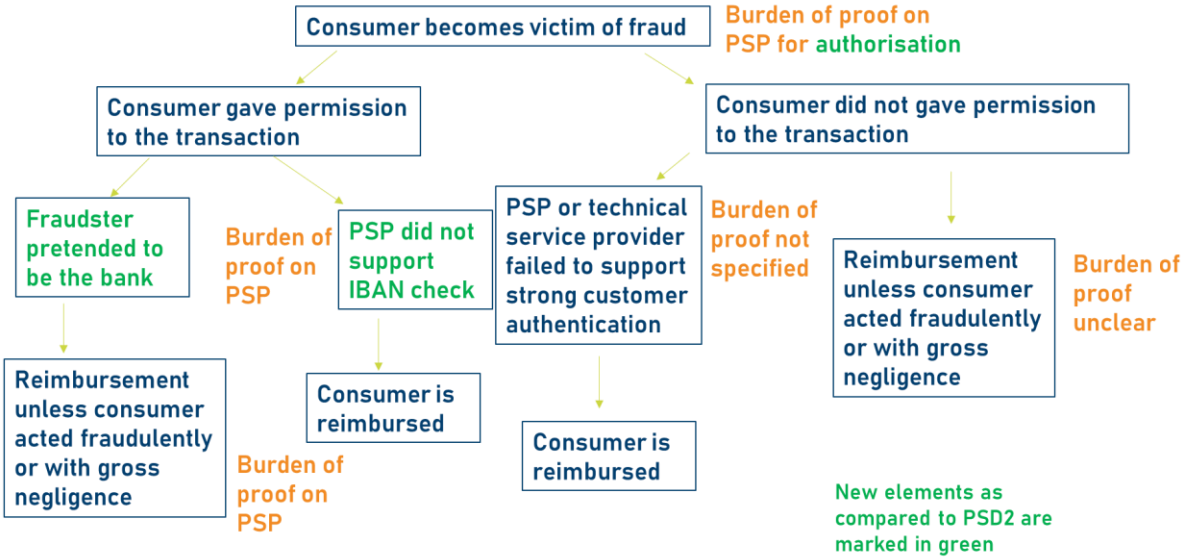
The burden to prove that a consumer acted fraudulently or with gross negligence should be on the payment service provider for all authorised and unauthorised transactions. For consumers, it will be impossible to prove that they did **not** act fraudulently or with gross negligence. PSPs shall document where they have stipulated that a consumer was acting fraudulently or with gross negligence and report this data as part of their annual fraud reporting to the competent authority to allow for structural enforcement measures. A mere presumption of "gross negligence" (prima facie evidence) should be ruled out as invalid. Gross negligence must be interpreted as an exceptional situation where a consumer acted with a "significant degree of carelessness" as indicated in recital 82. Where fraud cases are known to the PSP (see next paragraph on information sharing), it should not be possible to hold consumers liable due to "gross negligence".

[3] EBA (2022): Discussion paper on the EBA's preliminary observations on selected payment fraud data under PSD2, as reported by the industry. Available here: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Discussions/2022/Discussion%20Paper%20on%20the%20payment%20fraud%20data%20received%20under%20PSD2/1026061/Discussion%20Paper%20on%20the%20EBA%27s%20preliminary%20observations%20on%20selected%20payment%20fraud%20data%20under%20PSD2%20as%20reported%20by%20the%20industry.pdf

[4] Which? (2023): New rules to protect cash access and scam victims become law. Available here: https://www.which.co.uk/news/article/new-rules-to-protect-cash-access-and-scam-victims-become-law-am2Qk6S6FavR?utm_medium=Email&utm_source=ExactTarget&utm_campaign=4256994-B2B_Impact%20Newsletter_060723&mi_u=211817211&mi_ecmp=B2B_Impact+Newsletter_060723

[5] Push payments are payments where the consumer initiates the payment, for example credit transfers. Conversely pull payments are initiated by the payee, for example card payments.

INFOGRAPHIC: Liability regime in the Payment Services Regulation



Consumers can now flag to PSPs where an IBAN was used for fraudulent credit transfers. PSPs **can** share this data with other PSPs via information sharing arrangements. BEUC supports the concept of information sharing but would like to further improve it. PSPs should be liable without exemptions if a fraud case involves this IBAN number after the warning has been received. In addition, information sharing arrangements shall become mandatory to render them more efficient. Not only individual consumers, but also consumer organisations should be able to flag fraud cases as they often receive such information via their consumer helplines or systematically track these cases.[6] Social media platforms and search engines, without prejudice to their obligations under the Digital Services Act and the Unfair Commercial Practices Directive, should be obliged to cooperate with PSPs to delete content where this has been identified as the origin of the fraud case (e.g. advertising for fake shops, search engine results listing fake online banking websites). PSPs should be obliged to share this information with platforms under the established procedure of the Digital Services Act (Article 16 DSA and subsequent articles). Therefore, a clear link between the information sharing arrangements and the DSA must be established. In addition, to ease implementation, it would be helpful to clearly define what must be considered as a "fraudulent" IBAN and which checks and actions must be undergone by the PSP once the warning has been received.

Consumers should receive more possibilities to prevent fraud. Customer services shall be available via different channels (including a 24/7 telephone line) to block a payment instrument or a transaction.[7] If the customer service is unavailable, the consumer shall not be liable for the financial loss. In addition, consumers should be allowed to set spending limits which they cannot change in their online banking and set the possibility to apply a change in spending limits only after a certain time (e.g. 24 hours). Consumers should also

[6] Systematic tracking of fraud cases, is done for example by the Danish Consumer Council (here) and the Watchlist Internet in Austria (here).

[7] Vzbv (2023): Im Notfall schwer erreichbar. Erhebung zu telefonischen Kontaktmöglichkeiten bei Neobanken und Direktbanken. Available here: https://www.vzbv.de/sites/default/files/2023-07/23-05-10_Ergebnispapier_ServicetelefoneNeobanken_final.pdf

always have the possibility to opt for a slower credit transfer (with more possibilities to block a transaction), for example for new beneficiaries. This will help especially vulnerable consumers to use online banking services in a more secure way and prevent them from taking hasty actions under the psychological pressure of fraudsters.

As regards consumer education, PSPs should develop a coherent approach in their communication towards consumers. For instance, warnings like "your bank will never send you an e-mail" are only effective if the PSP is indeed never communicating by e-mail. Payment initiation providers relying on a path with multiple TANs or asking consumers to enter security credentials on their website undermine warnings saying that credentials should never be shared with third parties or where several TANs are required, consumers should stop the procedure due to fraud risks.

Which? study: The psychology of scams: how fraudsters trick their victims

Which? conducted in-depth interviews with fraud victims to learn how and why the fraud happened. The results of the study show that consumers do not act carelessly and even questioned the scammer but still got defrauded due to advanced manipulation tactics:

- Spoofing numbers from authorities, families or friends of the victim
- Credible online profiles (e.g. professional websites)
- Knowledge of past payment transactions of the victim's account

combined with psychological tricks such as creating a sense of urgency and often a stressful situation in the personal life of the consumer. When realising that they have been defrauded, victims feel ashamed and lengthy procedures with their banks add further distress.

The results indicate that it is not negligence on consumers' behalf causing the fraud but rather sophisticated techniques by professional fraudsters which are hard to detect. More systematic reimbursement will not reduce the level of care as the psychological stress of losing money remains but will bring fairer treatment of fraud victims. Read more: https://www.which.co.uk/policy-and-insight/article/the-psychology-of-scams-aizJj8F0E4rY#thescam

5. Enforcement

The introduction of new investigation powers for competent authorities and mandatory rules on administrative sanctions are important steps towards more structural enforcement. To allow investigations to be successful, PSPs shall be obliged to maintain adequate documentation when stipulating for example that consumers have acted fraudulently or with gross negligence in a fraud case.

What is, however, missing in the proposal are remedies for the harm to consumers for example when PSPs reimbursed consumers too late or wrongly stipulated that consumers where acting with "gross negligence" in a fraud case, where consumers lose money due to

the omission of information on charges for money remittances or where their data is leaked in the context of open banking.

In addition, PSPs should be obliged to participate in alternative dispute resolution and to accept the outcomes of such procedures. Currently, consumers often have to rely on lengthy and costly court procedures as PSPs refuse to participate in ADR or refuse to accept the solution found by the mediator. As shown in the annual report of the Belgian ombudsman (Ombudsfin), for the topic of online payment fraud, 62.2% of cases were not solved due to a refusal from the payment service provider to participate in ADR.[8]

UFC Que Choisir: Banks systematically refuse to reimburse consumers

In 2022, UFC Que Choisir launched a complaint against 12 banks and 'neobanks' in France based on 4,300 cases of payment fraud. 60% of the cases concerned fraud sums above €4,000.

The cases reveal that banks systematically refuse to reimburse consumers claiming that they have acted with "gross negligence" or have authorised the payment without bringing any proof that the consumer was indeed grossly negligent or at the origin of the payment.

Following this case, the French government adopted a law which foresees remedies for consumers in case PSPs reimburse them late. In the PSR, remedies are so far not foreseen and should be added in the proposal to ensure fair treatment of fraud victims.
Read more: https://www.quechoisir.org/action-ufc-que-choisir-refus-de-remboursement-des-fraudes-bancaires-l-ufc-que-choisir-depose-plainte-contre-12-banques-n101896/

6. Supervision

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 is suboptimal for enforcement as payment service providers can choose the Member State with the most liberal regime. In addition, Member States have limited possibilities to take action in their country as they are not responsible for payment service providers who registered elsewhere, and consumers will struggle to file complaints as they need to address a competent authority in another country.

Instead, 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.

[8] Ombudsfin, Rapport annuel 2022, available here : https://www.ombudsfin.be/sites/default/files/Ombudsfin-FR.pdf, p. 9.

Translated to payment services, a payment institution gets authorised in one Member State (home Member State) and the host Member State (where the PSP operates) will have day-to-day supervisory powers and enabled to take all necessary measures in case of breaches of 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.

7. To go further on the topic

- BEUC position paper: Review of the Payment Services Directive 2 – BEUC recommendations: https://www.beuc.eu/sites/default/files/publications/BEUX-X-2022-118_BEUC_position_paper_on_PSD2_review.pdf
- BEUC position paper: Consumer-friendly Open Banking – Access to consumers' financial data by third parties: https://www.beuc.eu/sites/default/files/publications/beuc-x-2018-082_consumer-friendly_open_banking.pdf
- BEUC position paper: BEUC's recommendations to the EDPB on the interplay between the GDPR and PSD2: https://www.beuc.eu/sites/default/files/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf
- BEUC factsheet: A payment fraud epidemic – what's the remedy for consumers: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-027_A_payment_fraud_epidemic.pdf
- Infographic payment fraud: How hackers get around strong authentication: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-036_How_hackers_get_around_strong_authentication.pdf
- AGE-BEUC Factsheet: Everyone needs to make payments – The importance of inclusive payment methods: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-044_The_importance_of_inclusive_payment_methods.pdf

END

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.