

Public consultation on the review of the revised payment services Directive (PSD2) and on open finance

Fields marked with * are mandatory.

Introduction

This consultation is available in all European Union official languages.

Please use the language selector at the top of this page to choose your language for this consultation.

Purpose and structure of the consultation

The Commission is launching this public consultation to gather evidence for the PSD2 review and to inform its work on open finance. It targets the public, and no in-depth knowledge of PSD2 or open finance is required. It is available in all official EU languages.

As well as this public consultation, two targeted consultations will be launched, one [targeted consultation on the review of PSD2](#) and the [targeted consultation on the open finance framework](#). These consultations will have more detailed questions that require specific knowledge of payment services, the PSD2, and data sharing in the financial sector. These targeted consultations are only available in English.

We invite you to respond to

- **this public consultation** if you have little knowledge about the payments industry and the relevant laws
- one or both of the **targeted consultations** if you are a professional stakeholder in the payments industry, e.g. you are a payment institution employee, represent a financial institution members' association, or are knowledgeable about payments

The results of all the consultations will inform the PSD2 review and open finance policy. The results may also serve as input for impact assessments accompanying any possible legislative proposals revising the PSD2 or putting in place an open finance framework.

In addition to answering to the questions raised in this online survey, you can add any useful documents and /or data (this can be done at the end of this questionnaire).

Please give concrete examples in your answers when possible. Where appropriate, please make specific operational suggestions to the questions raised. This will support the review process.

Background

The [revised Payment Services Directive \(Directive 2015/2366/EC\)](#) is the basis for payment rules in the EU. The [first Payment Services Directive](#), adopted in 2007, was revised to modernise rules due to increased digitalisation of payments and the emergence of new payment services providers and types of payment services. The Directive became applicable in January 2018, except for some rules on strong customer authentication (SCA) and access to payment accounts, which apply since September 2019.

PSD2 includes rules to

- make it easier and safer to use online payment services
- better protect payment services users against fraud, abuse, and payment problems
- promote innovative payment services
- strengthen the rights of payment services users

PSD2 sets out the conditions under which digital payments are to be executed. For example

- how long it should take for an account to be credited (execution time)
- whether there are fees associated with the transaction
- safety measures to be applied to ensure the security of the payment
- the liability regime in the event of unauthorised access (fraud), i.e. who is responsible
- how to file complaints

PSD2 focuses on digital payments, e.g. non-cash payments using payment instruments such as cards, credit transfers, direct debits, etc. that can be made in person or via online banking, e.g. via a mobile phone.

Since the adoption of PSD2, the payments market has continued to evolve with new players entering the market, more advanced payments technologies (such as contactless) emerging, and payments needs changing. These market changes warrant an in-depth analysis.

The review aims to assess the effectiveness, efficiency, costs and benefits, coherence and the EU added value of the Directive. It will determine if the PSD2 objectives have been achieved or if changes are needed (and if so, the type and scope of changes). Any forward-looking aspects will also consider the Commission's ongoing work on the open finance framework.

The review will have two dimensions. It will be backward-looking (evaluating the application and impact of the Directive) and forward-looking (assessing the need for possible legislative amendments ensuring that EU retail payment rules remain fit for purpose and future-proof).

As regards open finance, the revised PSD2 opened up access to customers' payment accounts data, enabling third-party information and financial service providers to reuse this data with the customer's agreement. The general purpose of this data reuse was to offer competing financial services or information services, such as comparison tools and data aggregation across several providers. Thus, the PSD2 effectively laid the ground for 'open banking', or the principle of third-party access to customer data in the area of banking products and services. Open finance as a concept is broader and goes beyond the scope of payments account data in the revised PSD2, as it could cover a range of financial services, such as investment in securities, pensions and insurance.

In 2020, the Commission set data-driven finance as one of the priorities in its [digital finance strategy](#) and announced an open finance framework legislative proposal. As reiterated in the [capital markets union \(CMU\) Communication of November 2021](#), the Commission is now accelerating this work as an integral part of the European financial data space. In the broader framework of the [data strategy for Europe](#), the objective is to make the most of the data economy for EU capital markets, consumers and businesses. Building on the PSD2, this will ensure that more data are available for innovative financial services. It will also give consumers more choice and help them find products that best fit their investment preferences (including sustainable products), while continuing to give them control of their data, including who can access it. This should directly contribute to increasing retail investment.

Please note: In order to ensure a fair and transparent consultation process **only responses received through our online questionnaire will be taken into account** and included in the report summarising the responses. Should you have a problem completing this questionnaire or if you require particular assistance, please contact fisma-psd2-review@ec.europa.eu.

More information on

- [this consultation](#)
- [the consultation document](#)
- [the related call for evidence on the review of PSD2](#)
- [the related targeted consultation on the review of PSD2](#)
- [the related call for evidence on the open finance framework](#)
- [the related targeted consultation on the open finance framework](#)
- [payments services](#)
- [the protection of personal data regime for this consultation](#)

About you

* Language of my contribution

- Bulgarian
- Croatian
- Czech
- Danish

- Dutch
- English
- Estonian
- Finnish
- French
- German
- Greek
- Hungarian
- Irish
- Italian
- Latvian
- Lithuanian
- Maltese
- Polish
- Portuguese
- Romanian
- Slovak
- Slovenian
- Spanish
- Swedish

* I am giving my contribution as

- Academic/research institution
- Business association
- Company/business organisation
- Consumer organisation
- EU citizen
- Environmental organisation
- Non-EU citizen
- Non-governmental organisation (NGO)
- Public authority
- Trade union
- Other

* First name

STEFAN

* Surname

VOICU

* Email (this won't be published)

voicu@betterfinance.eu

* Organisation name

255 character(s) maximum

BETTER FINANCE - European Federation of Investors and Financial Services Users

* Organisation size

- Micro (1 to 9 employees)
- Small (10 to 49 employees)
- Medium (50 to 249 employees)
- Large (250 or more)

Transparency register number

255 character(s) maximum

Check if your organisation is on the [transparency register](#). It's a voluntary database for organisations seeking to influence EU decision-making.

24633926420-79

* Country of origin

Please add your country of origin, or that of your organisation.

- | | | | |
|--------------------------------------|--|-------------------------------------|--|
| <input type="radio"/> Afghanistan | <input type="radio"/> Djibouti | <input type="radio"/> Libya | <input type="radio"/> Saint Martin |
| <input type="radio"/> Åland Islands | <input type="radio"/> Dominica | <input type="radio"/> Liechtenstein | <input type="radio"/> Saint Pierre and Miquelon |
| <input type="radio"/> Albania | <input type="radio"/> Dominican Republic | <input type="radio"/> Lithuania | <input type="radio"/> Saint Vincent and the Grenadines |
| <input type="radio"/> Algeria | <input type="radio"/> Ecuador | <input type="radio"/> Luxembourg | <input type="radio"/> Samoa |
| <input type="radio"/> American Samoa | <input type="radio"/> Egypt | <input type="radio"/> Macau | <input type="radio"/> San Marino |
| <input type="radio"/> Andorra | <input type="radio"/> El Salvador | <input type="radio"/> Madagascar | <input type="radio"/> São Tomé and Príncipe |

- Angola
- Anguilla
- Antarctica
- Antigua and Barbuda
- Argentina
- Armenia
- Aruba
- Australia
- Austria
- Azerbaijan
- Bahamas
- Bahrain
- Bangladesh
- Barbados
- Belarus
- Belgium
- Belize
- Benin
- Bermuda
- Bhutan
- Bolivia
- Bonaire Saint Eustatius and Saba
- Bosnia and Herzegovina
- Botswana
- Bouvet Island
- Brazil
-
- Equatorial Guinea
- Eritrea
- Estonia
- Eswatini
- Ethiopia
- Falkland Islands
- Faroe Islands
- Fiji
- Finland
- France
- French Guiana
- French Polynesia
- French Southern and Antarctic Lands
- Gabon
- Georgia
- Germany
- Ghana
- Gibraltar
- Greece
- Greenland
- Grenada
- Guadeloupe
- Guam
- Guatemala
- Guernsey
- Guinea
- Guinea-Bissau
- Malawi
- Malaysia
- Maldives
- Mali
- Malta
- Marshall Islands
- Martinique
- Mauritania
- Mauritius
- Mayotte
- Mexico
- Micronesia
- Moldova
- Monaco
- Mongolia
- Montenegro
- Montserrat
- Morocco
- Mozambique
- Myanmar/Burma
- Namibia
- Nauru
- Nepal
- Netherlands
- New Caledonia
- New Zealand
- Nicaragua
- Saudi Arabia
- Senegal
- Serbia
- Seychelles
- Sierra Leone
- Singapore
- Sint Maarten
- Slovakia
- Slovenia
- Solomon Islands
- Somalia
- South Africa
- South Georgia and the South Sandwich Islands
- South Korea
- South Sudan
- Spain
- Sri Lanka
- Sudan
- Suriname
- Svalbard and Jan Mayen
- Sweden
- Switzerland
- Syria
- Taiwan
- Tajikistan
- Tanzania
- Thailand

- British Indian Ocean Territory
- British Virgin Islands
- Brunei
- Bulgaria
- Burkina Faso
- Burundi
- Cambodia
- Cameroon
- Canada
- Cape Verde
- Cayman Islands
- Central African Republic
- Chad
- Chile
- China
- Christmas Island
- Clipperton
- Cocos (Keeling) Islands
- Colombia
- Comoros
- Congo
- Cook Islands
- Costa Rica
- Côte d'Ivoire
- Croatia
-
- Guyana
- Haiti
- Heard Island and McDonald Islands
- Honduras
- Hong Kong
- Hungary
- Iceland
- India
- Indonesia
- Iran
- Iraq
- Ireland
- Isle of Man
- Israel
- Italy
- Jamaica
- Japan
- Jersey
- Jordan
- Kazakhstan
- Kenya
- Kiribati
- Kosovo
- Kuwait
-
- Niger
- Nigeria
- Niue
- Norfolk Island
- Northern Mariana Islands
- North Korea
- North Macedonia
- Norway
- Oman
- Pakistan
- Palau
- Palestine
- Panama
- Papua New Guinea
- Paraguay
- Peru
- Philippines
- Pitcairn Islands
- Poland
- Portugal
- Puerto Rico
- Qatar
- Réunion
- Romania
-
- The Gambia
- Timor-Leste
- Togo
- Tokelau
- Tonga
- Trinidad and Tobago
- Tunisia
- Turkey
- Turkmenistan
- Turks and Caicos Islands
- Tuvalu
- Uganda
- Ukraine
- United Arab Emirates
- United Kingdom
- United States
- United States Minor Outlying Islands
- Uruguay
- US Virgin Islands
- Uzbekistan
- Vanuatu
- Vatican City
- Venezuela
- Vietnam
-

- | | | | |
|--|----------------------------------|---|---|
| <input type="radio"/> Cuba | <input type="radio"/> Kyrgyzstan | <input type="radio"/> Russia | <input type="radio"/> Wallis and Futuna |
| <input type="radio"/> Curaçao | <input type="radio"/> Laos | <input type="radio"/> Rwanda | <input type="radio"/> Western Sahara |
| <input type="radio"/> Cyprus | <input type="radio"/> Latvia | <input type="radio"/> Saint Barthélemy | <input type="radio"/> Yemen |
| <input type="radio"/> Czechia | <input type="radio"/> Lebanon | <input type="radio"/> Saint Helena
Ascension and
Tristan da Cunha | <input type="radio"/> Zambia |
| <input type="radio"/> Democratic
Republic of the
Congo | <input type="radio"/> Lesotho | <input type="radio"/> Saint Kitts and
Nevis | <input type="radio"/> Zimbabwe |
| <input type="radio"/> Denmark | <input type="radio"/> Liberia | <input type="radio"/> Saint Lucia | |

* Field of activity or sector (if applicable)

- Accounting
- Auditing
- Banking
- Credit rating agencies
- Insurance
- Pension provision
- Investment management (e.g. hedge funds, private equity funds, venture capital funds, money market funds, securities)
- Market infrastructure operation (e.g. CCPs, CSDs, Stock exchanges)
- Social entrepreneurship
- Other
- Not applicable

* Please specify your activity field(s) or sector(s)

Retail financial services users

The Commission will publish all contributions to this public consultation. You can choose whether you would prefer to have your details published or to remain anonymous when your contribution is published. **For the purpose of transparency, the type of respondent (for example, 'business association', 'consumer association', 'EU citizen') country of origin, organisation name and size, and its transparency register number, are always published. Your e-mail address will never be published.** Opt in to select the privacy option that best suits you. Privacy options default based on the type of respondent selected

* **Contribution publication privacy settings**

The Commission will publish the responses to this public consultation. You can choose whether you would like your details to be made public or to remain anonymous.

Anonymous

Only organisation details are published: The type of respondent that you responded to this consultation as, the name of the organisation on whose behalf you reply as well as its transparency number, its size, its country of origin and your contribution will be published as received. Your name will not be published. Please do not include any personal data in the contribution itself if you want to remain anonymous.

Public

Organisation details and respondent details are published: The type of respondent that you responded to this consultation as, the name of the organisation on whose behalf you reply as well as its transparency number, its size, its country of origin and your contribution will be published. Your name will also be published.

I agree with the [personal data protection provisions](#)

Payment methods

Question 1. How do you usually pay for goods and services?

For each payment method, please indicate how often you use it

a) In a physical shop:

	1 (preferred option)	2 (sometimes)	3 (never)	Don't know - No opinion - Not applicable
Cash	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Payment card (debit or credit)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Digital wallet on mobile phone	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Other payment solutions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

b) Online:

--	--	--	--	--

	1 (preferred option)	2 (sometimes)	3 (never)	Don't know - No opinion - Not applicable
Payment card (debit or credit)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Digital wallet on mobile phone	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Digital wallet on PC or laptop	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Bank transfer	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Other payment solutions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Question 2. The Payment Services Directive aims to promote innovative internet-based and mobile payment services.

Do you think that the payments market is innovative enough?

- Yes
- No
- Don't know / no opinion / not applicable

Question 2.1 Please explain why you don't think the payments market is innovative enough:

1000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The payments market is fragmented: there are certain countries in the EU/EEA where the use of digital payments is more often (e.g. Iceland, Belgium), and the markets is more developed, whereas in other countries cash is still the main form of payment.

In recent years, **new payment service providers** have entered the market. Many are not banks, and they include big tech companies (i.e. large online platforms offering search engines, social networking services and more).

Question 3.1 Do you believe that you have a larger choice of payment services than you did 5 years ago?

- Yes
-

- No, I have the same choice as before
- No, I have less choice
- Don't know / no opinion / not applicable

Question 3.2 What do you think about new companies, including big tech companies, entering the payments market?

1000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

By default, the clients' (data subjects') data should not be retained further than what is strictly necessary for the provision of the service and afterwards deleted.

To use these services, payment service providers need access to your payment account(s) data, which requires your consent. There are two kinds of providers

- **Account information services providers (AISP):** these access data from your online accessible payment account(s) and consolidate these data to, for example, help you manage your finances
- **Payment initiation services providers (PISP):** these provide an online service that accesses your payment account to transfer funds on your behalf with your consent and authentication. For example, you could have payment accounts from different banks together in a PISP app on your phone and transfer funds from any of those payment accounts directly from the app

AISPs and PISPs do not actually handle your funds. Once they have your consent, AISPs get access to your transaction history, and PISPs facilitate the payment, but they never come into possession of your funds.

Question 3.3 Do you use AISPs and/or PISPs?

- I only use AISP(s)
- I only use PISP(s)
- I use both AISPs and PISPs
- I don't use any of them
- Don't know / no opinion / not applicable

Digital payments

Question 4. Do you make digital payments?

- Yes
- No
- Don't know / no opinion / not applicable

An important objective of the Payment Services Directive was to make digital payments (non-cash payments using electronic payment instruments, e.g. payment cards, mobile phones, etc.) and online banking safer and easier for consumers.

Question 4.1 Based on your experience with digital payments over the last 5 years, please indicate to what extent you agree with the following statements:

	1 (strongly agree)	2 (somewhat agree)	3 (neutral)	4 (somewhat disagree)	5 (strongly disagree)	Don't know - No opinion - Not applicable
Making digital payments has become easier	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
It has become easier to make digital payments to other EU countries (e.g. when buying from an online shop in another EU country)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
It has become easier to make digital payments to non-EU countries (e.g. when buying from an online shop in a non-EU country)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
It has become easier to transfer money to other EU countries	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
It has become easier to transfer money to non-EU countries	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

The Payment Services Directive includes measures to protect consumers. Some examples are described below (please note that the below is not an exhaustive list)

- Transparency: before and after transactions have been executed, payment service providers must inform users about all fees payable, when the transaction will be completed, etc.
- Rights and obligations: for some unauthorised payment transactions, the Directive has limited the liability of the payer, for example, when a payment card is lost
- Fraud prevention: PSD2 introduced strong customer authentication (SCA, see explanation below) for making payment transactions or giving access to payment accounts

The following questions ask your opinion on consumer protection and the Payment Services Directive.

Question 4.2 Please indicate to what extent you agree with the following statements about information and fees:

	1 (strongly agree)	2 (somewhat agree)	3 (neutral)	4 (somewhat disagree)	5 (strongly disagree)	Don't know - No opinion - Not applicable
Before paying (either online or in a physical shop), I know if I will have to pay a fee in addition to the price of the product(s) or service(s) purchased	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The cost of any fees is always clear	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
If a payment includes a currency conversion (e.g. from euro to Swedish Krona), it is always clear what exchange rate will be applied	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
When charged with fees for ATM cash withdrawals, it is always clear what these fees are	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
When withdrawing cash abroad at an ATM in another currency, it is always clear what exchange rate will be applied	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
The information I receive before I make a payment is sufficient	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 4.2.1 If you find that the information provided to you during a payment transaction or cash withdrawal is not always clear, please explain what is not clear?

1000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

In currency conversation online transactions and for ATM withdrawals outside of the home country, the amount of fees charged are not always clear for the consumer, nor is the currency conversion rate. In addition, these procedures should show the rate at which currency is exchanged vs the central bank rate of the day.

Question 4.2.2 Do you require additional information before making a payment?

- Yes
- No
- Don't know / no opinion / not applicable

Please explain what additional information you need before making a payment:

750 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

See question above.

To make payment transactions more secure and prevent fraud further, the Payment Services Directive introduced strong customer authentication (SCA or '2-factor authentication'). This requires authentication through a combination of two of the following three factors: 'something I possess' (e.g. card, mobile phone), 'something I know' (e.g. PIN), or 'something I am' (e.g. fingerprints).

Making a payment, either in a physical shop or online, usually involves SCA (except in certain circumstances, e.g. low-value contactless payments). SCA can be done using a mobile phone or through other means, such as card reader or a code-generating device.

Question 4.3 What is your opinion about confirming your payment with SCA?

a) When buying something in a physical shop:

- It is easy, and I have no problem with it
- It is cumbersome, but I accept it because it protects me against fraudsters
- It is cumbersome, and I do not see the point of it

- Other
- Don't know / no opinion / not applicable

Please specify to what is your opinion about confirming your payment with SCA when buying something in a physical shop:

750 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Generally, SCA are easy but it depends on the card provider. Most users do not face issues, although certain users who are not as digitally literate may face difficulties.

b) When buying something online:

- It is easy, and I have no problem with it
- It is cumbersome, but I accept it because it protects me against fraudsters
- It is cumbersome, and I do not see the point of it
- Other
- Don't know / no opinion / not applicable

Please specify to what is your opinion about confirming your payment with SCA when buying something online:

750 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Same as above

Payment service providers are required to implement SCA and can decide how to implement it. They usually enable SCA via a mobile phone app and/or another specific device.

Question 4.3.1 Besides payments made on mobile phones, do you think payment service providers should be required to offer SCA solutions other than through mobile phones?

- Yes
- No
- Don't know / no opinion / not applicable

Question 4.3.2 Do you believe payment service providers should put in place more security measures?

- Yes
- No
- Don't know / no opinion / not applicable

Please explain your answer to question 4.3.2 and include any suggestions:

1000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Too many security measures can make online payments cumbersome: it would be easier if providers would implement "safety by design" features.

Since the COVID-19 pandemic, the number of contactless payments has increased significantly. The maximum amount for contactless payment transactions without SCA was increased to EUR 50 by payment service providers in most countries.

Question 4.4.1 What do you think about the maximum amount for a contactless payment (without SCA)?

If the euro is not the main currency in your country of residence, please convert EUR 50 to your local currency and select an answer:

- The EUR 50 limit should remain
- The limit should be lower than EUR 50
- The limit should be higher than EUR 50
- I should be able to set my own limit
- Other
- Don't know / no opinion / not applicable

Please specify to what other view(s) you have on the maximum amount for a contactless payment (without SCA):

750 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The limit at EUR 50 should be set by default but it should be mandatory for all PSP to allow users to modify the limit.

There is also a limit to the cumulative value of contactless payments, which differ by country. For example, in Germany, one must enter a PIN every three to five transactions or when a total of EUR 150 has been spent. In Czechia, a PIN is required for every third consecutive transaction.

Question 4.4.2 What is your opinion about this cumulative limit for contactless payments (without SCA)? Please give one answer for the value limit and one for the payments limit.

If the euro is not the main currency in your country of residence, please convert EUR 50 to your local currency and select an answer for 'Value in euro':

a) Value in euro:

- The limit should be lower than EUR 150
- The limit should be higher than EUR 150
- I should be able to set my own limit (including EUR 0)
- Other

Please specify to what other view(s) you have on the value limit for contactless payments (without SCA):

750 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Same as above.

b) Number of consecutive payments:

- This should be less than five consecutive payments
- This should be more than five consecutive payments
- I should be able to set my own limit (including zero payments)
- Other

Please specify to what other view(s) you have on the payments limit for contactless payments (without SCA):

750 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Same as above.

Blocking funds

For payments by card, funds can be blocked on your account if the exact final amount unknown at the time of payment. For example, when you are at an unmanned petrol station, you may have to agree to a certain amount of funds to be blocked before you fill up your tank. The blocked amount will then be corrected, and the exact final payment will be processed afterwards.

Question 4.5 Should there be a limit on the amount that can be blocked?

- Yes
- No, no limit is needed
- Other
- Don't know / no opinion / not applicable

Question 4.5.1 Please specify what you mean by "other" in your answer to question 4.5:

750 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The user should be able to change her/his limit.

Fraud

Question 4.6 As a consumer, have you been a victim of payment fraud recently?

- Yes
- No
- Don't know / no opinion / not applicable

Question 4.6.1 Please provide details on the payment fraud you have been a victim of:

2000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Many instances of fraud of consumers across the EU have been reported recently due to increased digital /online activity as a consequence of the global health pandemic. In most cases, however, PSPs make a whole refund to the consumer.

Question 4.6.2 If you were victim of a fraud did you ask your payment service provider for a refund?

- Yes, and I received a full refund
- Yes, but I only received a partial refund
- Yes, but I did not receive any refund
- Yes, but I requested a refund from another party
- No, I did not request a refund
- Don't know / no opinion / not applicable

Question 4.6.3 Were you satisfied with the refund process (requesting the refund, communication with your payment service provider, length of the process, etc.)?

1000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

A majority of consumers are satisfied.

Question 4.7 Please indicate to what extent you agree with the following statements about protection and security provided when making digital payments:

	1 (strongly agree)	2 (somewhat agree)	3 (neutral)	4 (somewhat disagree)	5 (strongly disagree)	Don't know - No opinion - Not applicable
Making digital payments has become more secure	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
My payments data is adequately protected	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Strong customer authentication has helped make digital payments safer and more secure	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
For digital payments, convenience and speed are more important than security	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 4.7.1 Please explain your answers and include any proposals you may have that further protect digital payments:

2000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Considering your responses to the questions above and that the payments market has many new players and technologies (including big tech companies and mobile phone payments):

Question 4.8.1 Do you have specific concerns about the payments market and recent market developments? For instance are there (new) risks that require special attention?

- Yes
- No
- Don't know / no opinion / not applicable

Please explain your answer to question 4.8.1:

2000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 4.8.2 What is your opinion about the level of regulation of the payments market? Is it sufficient or is there too much regulation? Please explain:

2000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Open finance

Open finance refers to a customer allowing their data to be shared or re-used by financial institutions and other third-party service providers to access a wider range of innovative services. It could cover different sets of data (business-to-business and business-to-consumer data) across a range of financial services (e.g. banking, insurance, investment, pensions). Consumers would be able to grant trusted third-party service providers access to their data, held by financial institutions or other service providers, in a safe and secure way until they decide to revoke their permission. As a result, consumers would have access to better or new services from these third-party service providers, including better-targeted financial advice, tools to manage their finances, and additional financial services. While the revised Payment Services Directive includes rules on such access for payment accounts (see previous sections of this consultation), no framework currently exists for other financial products.

Question 5. Would you be willing to share the following types of data held by your financial service provider (e.g. bank, insurance company, investment company) with other financial or third-party service providers to get access to new services (e.g. comparing offers, switching providers, financial services tailored to your situation and needs)?

	Yes	No	Don't know - No opinion - Not applicable
Savings account data	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Mortgage loan data	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Consumer credit data	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Securities account data	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Pension data	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Insurance data	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Please explain your answer to question 5:

750 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The question is biased and does not allow for balanced answers: as a matter of principle, data subjects' information use and transfer between financial services providers should be limited as much as possible. The principles enshrined in Art. 5 of GDPR and the consent validity rules of Art. 6 GDPR should be applied mutatis mutandis.

However, there can be use cases where sharing financial data from a larger pool of providers to one

particular provider may be beneficial (e.g. pension tracking systems). In these cases, however:

- the principles of purpose limitation and data minimisation should be strictly applied (Art. 5(1)(b) and (c) of GDPR)
- obtaining consent from the user must be explicitly prohibited for bundling services.

Question 6. Should financial service providers holding your data be obliged to share them with other financial or third-party service providers, provided that you have given your consent?

- Yes
- No
- Don't know / no opinion / not applicable

Question 7. Do you think there are security and/or privacy risks in giving other service providers access to your data?

- Yes
- No
- Don't know / no opinion / not applicable

Please explain your answer to question 7:

750 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 8. Do you think financial service providers that hold your data always ask for your consent before sharing those data with other financial or third-party service providers?

- Yes
- No
- Don't know / no opinion / not applicable

Question 9. If shared with another financial or third-party service provider, do you think these data are used exclusively for the purposes for which you have agreed?

- Yes
- No
- Don't know / no opinion / not applicable

Exchanging data between different service providers could be made more secure by putting in place a dedicated technical infrastructure for that purpose (e.g. a secure application programming interface).

Question 10. If service providers holding data put in place such infrastructure, do you think they should be able to charge a fee to other service providers who access data using this infrastructure?

- Yes
- No
- Don't know / no opinion / not applicable

Please explain your answer to question 10:

750 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

There should be an obligation to pass on part of the revenues directly to customers.

Additional information

Should you wish to provide additional information (e.g. a position paper, report) or raise specific points not covered by the questionnaire, you can upload your additional document(s) below. **Please make sure you do not include any personal data in the file you upload if you want to remain anonymous.**

The maximum file size is 1 MB.
You can upload several files.

Useful links

[More on this consultation \(https://ec.europa.eu/info/publications/finance-consultations-2022-psd2-review-open-finance_en\)](https://ec.europa.eu/info/publications/finance-consultations-2022-psd2-review-open-finance_en)

[Consultation document \(https://ec.europa.eu/info/files/2022-psd2-review-open-finance-consultation-document_en\)](https://ec.europa.eu/info/files/2022-psd2-review-open-finance-consultation-document_en)

[Related call for evidence on the review of PSD2 \(https://ec.europa.eu/info/law/better-regulation/initiatives/plan-2012798_en\)](https://ec.europa.eu/info/law/better-regulation/initiatives/plan-2012798_en)

[Related targeted consultation on the review of PSD2 \(https://ec.europa.eu/info/publications/finance-consultations-2022-psd2-review_en\)](https://ec.europa.eu/info/publications/finance-consultations-2022-psd2-review_en)

[Related call for evidence on the open finance framework \(https://ec.europa.eu/info/law/better-regulation/initiatives/plan-2021-11368_en\)](https://ec.europa.eu/info/law/better-regulation/initiatives/plan-2021-11368_en)

[Related targeted consultation on the open finance framework \(https://ec.europa.eu/info/publications/finance-consultations-2022-open-finance_en\)](https://ec.europa.eu/info/publications/finance-consultations-2022-open-finance_en)

[More on payments services \(https://ec.europa.eu/info/business-economy-euro/banking-and-finance/consumer-finance-and-payments/payment-services/payment-services_en\)](https://ec.europa.eu/info/business-economy-euro/banking-and-finance/consumer-finance-and-payments/payment-services/payment-services_en)

[Specific privacy statement \(https://ec.europa.eu/info/law/better-regulation/specific-privacy-statement_en\)](https://ec.europa.eu/info/law/better-regulation/specific-privacy-statement_en)

Contact

fisma-psd2-review@ec.europa.eu