Electronic Money Association
Crescent House
5 The Crescent
Surbiton, Surrey
KT6 4BN
United Kingdom
Telephone: +44 (0) 20 8399 2066
www.e-ma.org

European Data Protection Board
Rue Montoyer 30,
B-1000 Brussels

16 September 2020

Dear Sirs

Re: EMA response to Guidelines 06/2020 on the interplay of the second Payment Services Directive and the GDPR ("Guidelines")

The EMA is the EU trade body representing electronic money issuers and alternative payment service providers. Our members include leading payments and e-commerce businesses worldwide, providing online payments, card-based products, electronic vouchers, and mobile payment instruments. Most members operate across the EU, most frequently on a cross-border basis. A list of current EMA members is provided at the end of this document.

I would be grateful for your consideration of our comments and proposals.

Yours sincerely,

Thaer Sabri

Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

Response

Topics addressed in the Guidelines

The following topics are addressed in the draft Guidelines:

1. Explicit consent: Is GDPR explicit consent the same as PSD2 explicit consent?

2. Lawful grounds and further processing: What is the lawful basis for an ASPSP granting a TPP access to a payment account?

3. Silent party: On what lawful basis is the personal data of the silent party provided by the ASPSP to the AISP? Similarly, on what basis is the silent party's data accessed by the AISP?

4. Special categories of personal data; and

5. Data minimisation, security and transparency.

The EMA will address each of the above issues in this response. This response uses the abbreviations used in the Guidelines.

Preliminary EMA comments concerning the Introduction

The Guidelines have not used the definition of "Payment initiation service provider" ("**PISP**") from PSD2 consistently.

Paragraph 4 set out the definition of PISP as, "*[PISP] … refers to the provider of a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider*".

Paragraph 6 of the Guidelines provides:

"*PISPs provide services to initiate payment orders at the request of a payment service user with respect to **the user's** payment account held at another payment service provider*."

This statement is referenced with the definition from PSD 4(15).

However, PSD2 states "'*payment initiation service' ["**PIS**"] means a service to initiate a payment order at the request of the payment service user with respect to **a** payment account held at another payment service provider*" This is essentially the same as the definition of PIS that can be derived from paragraph 4 but different from the one that can be derived from paragraph 6.

This difference between the definition in paragraph 6 and PSD2 4(15) is significant, because a common PISP business model is to initiate payments on behalf of a merchant from the bank account of the merchant's customer.

In this case the PSU of the PISP is the payee, not the payer. The remaining text in the draft Guidance does not appear to take into account this model. Please note that PSD2 4(13) defines "payment order" not just in the context of the payer but also in the context of the payee – i.e. a "payment order" is "*an instruction by a payer or payee to its payment service provider requesting the execution of a payment transaction*".

We consider the definition of PISP from PSD2 should be used throughout the document in order to maintain consistency.

Issue 1: Lawful grounds and further processing: What is the lawful basis for an ASPSP granting a TPP access to a payment account?

Under PSD2, ASPSPs give TPPs access to personal data. On what legal basis can this information be shared?

1.1 Applicable articles:

RTS 36(1)(a) and (b):

Account servicing payment service providers shall comply with each of the following requirements:

(a)they shall provide account information service providers with the same information from designated payment accounts and associated payment transactions made available to the payment service user when directly requesting access to the account information, provided that this information does not include sensitive payment data;

(b) they shall, immediately after receipt of the payment order, provide payment initiation service providers with the same information on the initiation and execution of the payment transaction provided or made available to the payment service user when the transaction is initiated directly by the latter;

PSD2 66(1):

Member States shall ensure that a payer has the right to make use of a payment initiation service provider to obtain payment services as referred to in point (7) of Annex I. The right to make use of a payment initiation service provider shall not apply where the payment account is not accessible online.

PSD2 67(1):

Member States shall ensure that a payment service user has the right to make use of services enabling access to account information as referred to in point (8) of Annex I. That right shall not apply where the payment account is not accessible online.

GDPR 6(1)(c):

Processing shall be lawful only if and to the extent that at least one of the following applies:

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

1.2 Guidelines:

Paragraph 26:

The processing of personal data by the ASPSP consisting of granting access to the personal data requested by the PISP and AISP in order to perform their payment service to the payment service user is based on a legal obligation. In order to achieve the objectives of the PSD2, ASPSPs must provide the personal data for the PISPs´ and AISPs´ services, which is a necessary condition for PISPs and AISPs to provide their services and thus ensure the rights provided for in Articles 66(1) and 67(1) of the PSD2. Therefore, the applicable legal ground in this case is Article 6 (1) (c) of the GDPR.

1.3 EMA comment:

The EMA agrees with the position set out in the Guidelines.

Further processing

Are AISPs and PISPs restricted in their use of a PSU's personal data?

Can the AISP or PISP only use the payment service user's personal data for providing AIS or PIS respectively?

1.4 Applicable articles:

PSD2 66(3)(g):

The [PISP] shall […] not use, access or store any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer.

PSD2 67(2)(f):

*The [AISP] shall […] not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, **in accordance with data protection rules**.*

1.5 Guidelines:

Paragraph 11:

*Access to payment accounts and the use of payment account information is partly regulated in Articles 66 and 67 PSD2, which contain safeguards regarding the protection of (personal) data. Article 66 (3) (f) PSD2 states that the PISP shall not request from the payment service user any data other than those necessary to provide the payment initiation service, and Article 66 (3) (g) PSD2 provides that PISPs shall not use, access or store any data for purposes other than for performing the payment initiation service explicitly requested by the payment service user. Furthermore, Article 67 (2) (d) PSD2 limits the access of AISPs to the information from designated payment accounts and associated payment transactions, whereas Article 67 (2) (f) PSD2 states that AISPs shall not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules. **The latter emphasises that, within the context of the account information services, personal data can only be collected for specified, explicit and legitimate purposes. An AISP should therefore make explicit in the contract for what specific purposes personal account information data are going to be processed for, in the context of the account information service it provides.** The contract should be lawful, fair and transparent under Article 5 of the GDPR and also comply with other consumer protection laws.*

1.6 EMA comment:

The position of the PISP is clear. The PISP is limited to processing personal data for the PIS only. This is evident from the language of PSD2. However, the position of the AISP is different. In PSD2 67(2)(f), the phrase "in accordance with data protection rules" means that permitting the payment service user has given consent to the processing of their personal data in a manner compliant with the GDPR, the AISP is permitted to use the personal data used to provide the AIS in order to provide other types of services to the payment service user. It would be helpful if this paragraph 11 is redrafted to expressly state that AISPs may use personal data used to provide the AIS to provide other services, permitting the consent has been obtained in accordance with the GDPR.

The Guidelines appear to imply that all AISPs intend to process data for the same specific purposes. Please note that one payment service may comprise several purposes for processing personal data. Please further note that purposes for processing personal data will differ between AISPs as services offered by AISPs vary within the industry. We consider the Guidelines should take this into account.

Issue 2: Explicit consent: Is GDPR explicit consent the same as PSD2 explicit consent?

The PSD2 and the GDPR both contain the concept of "explicit consent". Does this term have the same meaning under each regime?

2.1 Applicable articles:

PSD2 94(2):

Payment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user.

GDPR 4(11):

'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

GDPR 9(2)(a):

'Explicit consent' is one of the exceptions from the general prohibition for processing special categories of personal data.

Guidelines 05/2020 on consent under Regulation 2016/679, EDPB, paragraph 93:

The term explicit refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent. An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement. Where appropriate, the controller could make sure the written statement is signed by the data subject, in order to remove all possible doubt and potential lack of evidence in the future.

2.2 Guidelines:

Paragraph 36:

"Explicit consent" referred to in Article 94 (2) PSD2 is a contractual consent. This implies that Article 94 (2) PSD2 should be interpreted in the sense that when entering a contract with a payment service provider under the PSD2, data subjects must be made fully aware of the specific categories of personal data that will be processed. Further, they have to be made aware of the specific (payment service) purpose for which their personal data will be processed and have to explicitly agree to these clauses. Such clauses should be clearly distinguishable from the other matters dealt with in the contract and would need to be explicitly accepted by the data subject.

2.3 EMA comment:

The Guidelines interpret the requirement of the PSP to obtain the "explicit consent" of the payment service user stated in PSD2 94(2) to mean the PSP must obtain the payment service user's consent by agreeing to contractual clauses. This interpretation restricts certain types of PSPs to provide services.

This interpretation does not pose a problem for PSPs providing payment services to a payment service user on continual basis. The continual provision of payment services is legislated for on a framework contract where contractual consent can be obtained by the payment service user agreeing to specific clauses in accordance with the Guidelines. For example, an issuer enters into a framework contract with a payment service user for the provision of the card and the payment services associated with the use of the card. The framework contract remains on foot whilst the payment services are provided to the payment service user. Accordingly, the contractual clauses containing the explicit consent language also remain valid for the duration of the contractual relationship. This interpretation does also not pose a problem for AISPs as AISPs are not subject to article 94(2) of PSD2 due to the express exclusion contained in PSD2 33(2).

In the context of a PISP providing a PIS to a merchant, which is the payee and not the payer in a payment transaction for the purchase of goods or services as discussed above, the interpretation that "explicit consent" means "contractual consent" means that the relevant payment service user for the purposes of PSD2 94(2) is the merchant (i.e. the payee) and not the consumer or another type of purchaser (i.e. the payer).

Such a PISP (that is one providing a PIS to a merchant) does not routinely enter into a contract with the payer because it provides its payment service to the merchant not the payer. A PISP enters into a contract with the payee and is, therefore, able to obtain the payee's "explicit consent" i.e. on the basis of the payee agreeing to certain clauses legislating for such consent in the framework contract. The Guidelines must not be misconstrued as requiring a PISP that provides its PIS to merchants to enter into contracts with a payer in order to obtain the payer's explicit consent, as this not required under PSD2 94(2) nor practically feasible. The payer does not enter into a contract with such a PISP. The payer has limited interaction with this type of PISP.

Such an interpretation would be incorrect and restrict the PISP's ability to comply with PSD2 94(2).

Issue 3: Silent party: On what basis is the personal data of the silent party provided by the ASPSP to the AISP? On what basis is the silent party's data accessed by the AISP?

ASPSPs must provide AISPs with the same information from the PSU's payment accounts and associated payment transactions that is made available to the PSU, provided this does not include sensitive payment data. The AISP will therefore not only have access to (personal) data related to the PSU, but also (personal) data related to third parties, so-called 'silent parties' (e.g. name and/or address and/or international bank account number of persons to whom the PSU recently transferred money, or from whom the PSU recently received money).

Is the ASPSP in breach? Is the AISP in breach?

3.1 Applicable articles:

RTS 36(1)(a) and (b):

Account servicing payment service providers shall comply with each of the following requirements:

(a)they shall provide account information service providers with the same information from designated payment accounts and associated payment transactions made available to the payment service user when directly requesting access to the account information, provided that this information does not include sensitive payment data;

(b) they shall, immediately after receipt of the payment order, provide payment initiation service providers with the same information on the initiation and execution of the payment transaction provided or made available to the payment service user when the transaction is initiated directly by the latter;

GDPR 5(1)(b):

Personal data shall be:

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

GDPR 6(1)(c):

Processing shall be lawful only if and to the extent that at least one of the following applies:

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

GDPR 6(1)(f):

1. *Processing shall be lawful only if and to the extent that at least one of the following applies:*

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

3.2 Guidelines:

Paragraph 46:

The GDPR may allow for the processing of silent party data when this processing is necessary for purposes of the legitimate interests pursued by a controller or by a third party (Article 6 (1)(f) GDPR). However, such processing can only take place when the legitimate interest of the controller is not "overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data".

Paragraph 47:

A lawful basis for the processing of silent party data by PISPs and AISPs - in the context of the provision of payment services under the PSD2 - could thus be the legitimate interest of a controller or a third party to perform the contract with the payment service user. The necessity to process personal data of the silent party is limited and determined by the reasonable expectations of these data subjects. In the context of providing payment services that are covered by the PSD2, effective and appropriate measures have to be established by all parties involved to safeguard that the interests or fundamental rights and freedoms of the silent parties are not overridden, and to ensure that the reasonable expectations of these data subjects regarding the processing of their personal data are respected. In this respect, the controller has to establish the necessary safeguards for the processing in order to protect the rights of data subjects. This includes technical measures to ensure that silent party data are not processed for a purpose other than the purpose for which the personal data were originally collected by PISPs and AISPs. If feasible, also encryption or other techniques must be applied to achieve an appropriate level of security and data minimisation.

3.3 EMA comment:

The EMA agrees with the position that an ASPSP provides the personal data of the silent party to the TPP on the basis of GDPR 6(1)(c) (necessary for compliance with a legal obligation).

The EMA further agrees with the position that the TPP may process the personal data of the silent party on the lawful basis set out in GDPR 6(1)(f) (legitimate interest of the controller) as the TPP has a legitimate interest to perform the contract with the payment service user.

Separately, please note there appears to be two conflicting statements in the Guidelines with respect to processing special category data with respect to the silent party.

Paragraph 49 of the Guidelines provides that consent of the silent party is not legally feasible:

With regard to further processing of silent party data on the basis of legitimate interest, the EDPB is of the opinion that these data cannot be used for a purpose other than that for which the personal data have been collected, other on the basis of EU or Member State law. ***Consent of the silent party is legally not feasible, because in order to obtain consent, personal data of the silent party would have to be collected or processed, for which no legal ground can be found under Article 6 GDPR.*** *The compatibility test of Article 6.4 of the GDPR cannot offer a ground for the processing for other purposes (e.g. direct marketing activities) either.*

Paragraph 56 of the Guidelines provides in cases where substantial public interest does not apply, obtaining the explicit consent of the silent party is the only remaining derogation available to process their special category data:

In cases where the derogation of article 9 (2) (g) GDPR does not apply, obtaining explicit consent in accordance with the conditions for valid consent in the GDPR, seems to remain the only possible lawful derogation to process special categories of personal data by TPPs.** The EDPB Guidelines 05/2020 on consent under Regulation 2016/679 states 31 that: "Article 9(2) does not recognize "necessary for the performance of a contract" as an exception to the general prohibition to process special categories of data. Therefore, controllers and Member States that deal with this situation should explore the specific exceptions in Article 9(2) subparagraphs (b) to (j). When service providers rely on Article 9 (2) (a) GDPR, they must ensure that they have been granted explicit consent before commencing the processing." Explicit consent as set out in Article 9 (2) (a) GDPR must meet all the requirements of the GDPR. **This also applies to silent party data.

We consider these two statements must be reconciled.

We further note the Guidelines do not address GDPR 11(1). GDPR 11(1) provides:

If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with [the GDPR].

Recital 57 GDPR explains GDPR 11(1) further:

If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of [the GDPR]. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller.

We consider the Guidelines should address the possibility for TPPs to avail of GDPR 11(1).

<u>Issue 4: Processing special categories of personal data</u>

The Guidelines indicate that transaction data can contain special categories of personal data. What derogations are available to process such data? What if there are no applicable derogations?

4.1 Guidelines Paragraph 51

At the same time, financial transactions can reveal sensitive information about individual data subject, including those related to special categories of personal data. For example, political opinions and religious beliefs may be revealed by donations made to political parties or organisations, churches or parishes. Trade union membership may be revealed by the deduction of an annual membership fee from a person's bank account. Personal data concerning health may be gathered from analysing medical bills paid by a data subject. Finally, information on certain purchases may reveal information concerning a person's sex life or sexual orientation. As shown by these examples even single transactions can contain special categories of personal data. Moreover, through the sum of financial transactions, different kinds of behavioural patterns could be revealed, including special categories of personal data and additional services that are facilitated by account information services might rely on profiling as defined by article 4 (4) of the GDPR. Therefore, the chances are considerable that a service provider processing information on financial transactions of data subjects also processes special categories of personal data.

4.2 EMA comment

The Guidelines assert, in summary, there is a considerable chance that transaction data includes special category data. We consider this assertion is to be overbroad. To determine whether transaction data contained special categories of data, each transaction would have to be considered individually. The Guidelines give the example of religious beliefs being revealed by donations to churches or parishes. Transacting with a church or parish does not indicate a person's religious beliefs, it merely indicates that a person transacted with a church or parish. It is possible to draw an assumption of a person's religious beliefs on the basis of a transaction, however, it is not conclusive and may be wrong. On the basis that it requires possibly incorrect assumptions to be drawn, we consider that transaction data should not be broadly considered to contain special categories of data.

Please note our comments above in relation to paragraph 56 of the Guidelines. For paragraph 57 of the Guidelines (technical measures to be implemented in the case of no available derogations), please see our comments to paragraph 63 below.

Issue 5: Data minimisation, security and transparency

5.1 Data minimisation

Paragraph 62:

When not all payment account data are necessary for the provision of the contract, a selection of the relevant data categories must be made by the AISP before the data are collected. For instance, data categories that may not be necessary may include the identity of the silent party and the transaction characteristics. Also, unless required by Member State or EU law, the IBAN of the silent party's bank account may not need to be displayed.

Paragraph 63:

In this respect, the possible application of technical measures that enable or support TPPs in their obligation to access and retrieve only the personal data necessary for the provision of their services could be considered, as part of the implementation of appropriate data protection policies, in line with article 24 (2) GDPR. In this respect, the EDPB recommends the usage of digital filters in order to support AISPs in their obligation to only collect personal data that are necessary for the purposes for which they are processed. For instance, when a service provider does not need the transaction characteristics (in the description field of the transaction records) for the provision of their service, a filter could function as a tool for TPPs to exclude this field from the overall processing operations by the TPP.

EMA comment:

The recommendation to restrict a TPP's access to information by means of a filter is inconsistent with the ASPSP's obligations set out in PSD2 and the RTS.

RTS 36(1)(a) and (b) provide as follows:

Account servicing payment service providers shall comply with each of the following requirements:

*(a)**they shall provide account information service providers with the same information from designated payment accounts and associated payment transactions made available to the payment service** user when directly requesting access to the account information, provided that this information does not include sensitive payment data;*

*(b) they shall, immediately after receipt of the payment order, provide payment initiation service providers **with the same information on the initiation and execution of the payment transaction provided or made available to the payment service user** when the transaction is initiated directly by the latter;*

The above articles provide that the ASPSP's obligation is, in summary, to provide the TPP with the same information that is made available to the PSU. Implementing a filter would result in the TPP being provided with less information than what is made available to the PSU and, therefore, the obligation set out in RTS 36(1)(a)(and (b) would not be fulfilled.

We note the qualification at the end of RTS 36(1)(a) that provides "*provided that this information does not include sensitive payment data*".

PSD2 4(32) provides:

'sensitive payment data' means data, including personalised security credentials which can be used to carry out fraud. For the activities of payment initiation service providers and account information service providers, the name of the account owner and the account number do not constitute sensitive payment data;

The rationale behind the recommendation to implement a filter does not appear to be to restrict the provision of sensitive payment data.

Paragraph 36 of the Guidelines provides:

For instance, when a service provider does not need the transaction characteristics (in the description field of the transaction records) for the provision of their service, a filter could function as a tool for TPPs to exclude this field from the overall processing operations by the TPP.

Here, the Guidelines recommend a filter is used to exclude the information indicated in the description field of a transaction record. Accordingly, the qualification at the end of RTS 36(1)(a) and (b) would not be a sufficient basis to restrict the information provided to the TPP in the manner set out in the Guidelines.

Please further note RTS 32(3):

Account servicing payment service providers that have put in place a dedicated interface ***shall ensure that this interface does not create obstacles to the provision of payment initiation and account information services****. Such obstacles, may include, among others, preventing the use by payment service providers referred to in Article 30(1) of the credentials issued by account servicing payment service providers to their customers, imposing redirection to the account servicing payment service provider's authentication or other functions, requiring additional authorisations and registrations in addition to those provided for in Articles 11, 14 and 15 of Directive (EU) 2015/2366, or requiring additional checks of the consent given by payment service users to providers of payment initiation and account information services.*

In short, RTS 32(3) requires ASPSP not to put in place a dedicated interface that creates "obstacles" to TPPs. A filter could be deemed an "obstacle" pursuant to RTS 32(2). We therefore consider this recommendation should be removed from the Guidelines.

5.2 Transparency and accountability

Paragraph 77:

The abovementioned Guidelines also clarify that controllers may choose to use additional tools to provide information to the individual data subject, such as privacy dashboards. A privacy dashboard is a single point from which data subjects can view 'privacy information' and manage their privacy preferences by allowing or preventing their data from being used in certain ways by the controller in question. A privacy dashboard could provide an overview of the TPPs that have obtained the data subjects explicit consent, and could also offer relevant information on the nature and amount of personal data that has been accessed by TPPs. In principle, an ASPSP may offer the user the possibility to withdraw a specific explicit PSD2 consent through the overview, which would result in a denial of access to their payment accounts to one or more TPPs. The user could also request an ASPSP to deny access to their payment account(s) to one or more particular TPPs, as it is the right of the user to (not) make use of an account information service. If privacy dashboards are used in order to give or withdraw an explicit consent, they should be designed and applied lawfully and in particular prevent creating obstacles to the TPPs right to provide services in accordance with the PSD2. In this respect and in accordance with the applicable provisions under the PSD2, a TPP has the possibility to obtain explicit consent from the user again after this consent has been withdrawn,

EMA comment:

We consider implementing a privacy dashboard could be effective permitting certain measures were put in place to ensure communication and transparency. Implementing a privacy dashboard should remain a recommendation only and be an available option for PSPs as a privacy dashboard may not be feasible in all cases.

When a PSU changes their privacy preferences with respect to a TPP, a message should be sent to the TPP immediately informing the TPP of the PSU's decision.

We consider it important TPPs are sufficiently identified on the privacy dashboard in order for the PSU to identify them. A PSU may be familiar with a TPP by its trading name, but not by the TPP's registered business name. Accordingly, where the TPP is identified by a name the PSU does not recognise, the PSU does not have sufficient information to manage their privacy preferences. In order to ensure the PSU is sufficiently informed to make decisions with respect to their privacy, we consider the Guidelines recommend privacy dashboards identify TPPs by their trading name in addition to their registered name.

Members of the EMA, as of September 2020

AAVE LIMITED
Account Technologies
Airbnb Inc
Airwallex (UK) Limited
Allegro Group
American Express
Azimo Limited
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network Ltd
Boku Inc
CashFlows
Ceevo
Circle
Citadel Commerce UK Ltd
Coinbase
Contis
Corner Banca SA
Crypto.com
Curve
eBay Sarl
ECOMMPAY Limited
Em@ney Plc
Euronet Worldwide Inc
Facebook Payments International Ltd
First Rate Exchange Services
Flex-e-card
Flywire
Gemini
Globepay Limited
GoCardless Ltd
Google Payment Ltd
IDT Financial Services Limited
Imagor SA
Ixaris Systems Ltd
Modulr FS Europe Limited
Moneyhub Financial Technology Ltd
MuchBetter
myPOS Europe Limited
Nvayo Limited
OFX
OKTO
One Money Mail Ltd
OpenPayd
Optal
Own.Solutions
Park Card Services Limited
Paydoo Payments UAB
Paymentsense
Payoneer
PayPal Europe Ltd
Paysafe Group
Plaid
PPRO Financial Ltd
PPS
Remitly
Revolut
SafeCharge UK Limited
Securiclick Limited
Skrill Limited
Soldo Financial Services Ireland DAC
Stripe
SumUp Limited
Syspay Ltd
Token.io
Transact Payments Limited
TransferMate Global Payments
TransferWise Ltd
TrueLayer Limited
Trustly Group AB
Uber BV
Vitesse PSP Ltd
Viva Payments SA
WEX Europe UK Limited
Wirecard AG
Wirex Limited
WorldFirst
Worldpay UK Limited
WorldRemit