**Electronic Money Association**
Crescent House
5 The Crescent
Surbiton
Surrey
KT6 4BN
United Kingdom
Telephone: +44 (0) 20 8399 2066
Facsimile: +44 (0) 870 762 5063
www.e-ma.org

**Jack Wilson**
Financial Conduct Authority
12 Endeavour Square
London E20 1JN
UK

12 October 2018

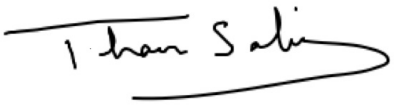
Dear Jack

**Re: EMA response to FCA CP 18/25 on the FCA Approach to final Regulatory Technical Standards and EBA guidelines under the revised Payment Services Directive (PSD2)**

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 that provide online payments, card-based products, electronic vouchers and mobile payment instruments. They also include a large number of smaller Payment Service Providers, including startups. The majority of EMA members are authorized in the UK, and 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 concerns.

Yours sincerely



Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

**EMA response to consultation**

**Q1: Do you agree with our approach to assessing requests for exemption to the contingency mechanism and our related guidance? If not, please explain why.**

The Electronic Money Association (EMA) finds that the FCA approach to assessing requests for exemption from the RTS requirement to build a contingency mechanism affords limited opportunity to Third Party Providers (TPPs) to communicate feedback on the design and testing of a dedicated interface. The FCA exemption assessment process appears to be based on the Exemption Request Form detailed in SUP 15C Annex1D. The 28 questions that are listed in the Form will enable Account Servicing Payment Service Providers (ASPSPs) to self-attest compliance with PSD2 & RTS requirements. It is not clear when/how the FCA proposes to seek feedback from the users of a dedicated interface (TPPs) that the interface has been designed and tested in accordance with RTS Art 30(2) to their satisfaction[1]. We propose that the FCA expands the exemption assessment process to seek feedback from TPPs that have registered to use the dedicated interface testing facility established by an ASPSP. The FCA should consider such feedback as part of the exemption assessment process.

We are also concerned that the FCA appears to consider conformance testing - related to the implementation of an API standard – a proxy of full compliance with PSD2/RTS requirements. Typically, such conformance testing only confirms compliance with a specific set of implementation requirements. The scope of these implementation requirements may well be more limited than the dedicated interface PSD2/RTS requirements. How does the FCA propose to verify that the conformance testing - carried out to confirm compliance of an interface with a set of API standard implementation requirements – fully covers the dedicated interface requirements detailed in *PSD2 and in the RTS on SCA and CSC*?

We would invite the FCA to provide more clarity on the success metrics of the exemption assessment process detailed in Section 1.22 of the Consultation paper "*We will also consider the number of successful exemption requests as an indicator of success*". Since, the FCA exemption assessment process adopts a weakened version of the *wide usage* RTS criterion[2], we would expect the FCA to also consider a range of quality success metrics. An example of a quality success

[1] See RTS Art. 33(6) (b).

[2] Aligned with Guideline 7 of the Draft *EBA Guidelines on the conditions to benefit from the contingency mechanism exemption*.

metric would be the scope of TPP use of exempted dedicated interfaces at the time of approval of an exemption request. A process whereby the FCA grants exemptions to large numbers of ASPSP dedicated interfaces that can only demonstrate availability of the interface testing facility/ documentation cannot deliver the payment account access outcomes intended by PSD2; in our mind, such an exemption request assessment process cannot be considered successful.

EMA members challenge the interpretation of the obstacles to the provision of TPP services detailed in Par 17.125. Specifically, the statement that "… *the SCA-RTS do not state that redirection per se is an obstacle for AISPs and PISPs*" when Redirection is explicitly listed as such an obstacle in RTS Art 32(3). The RTS text lists the imposition of redirection as an example of an obstacle among three other types of obstacles in a non-exhaustive list. The FCA appears to accept that all other items in that list (i.e. preventing the TPP use of PSCs issued by the ASPSP, requiring additional TPP authorisations and registrations, requiring additional checks of the PSU consent granted to the TPP) constitute obstacles as stated in Par 17.114. In that context, it is difficult to reconcile the FCA reasoning that the imposition of redirection as the only PSU authentication method that is available for use by TPPs does not constitute an obstacle, itself.

The imposition of the use of redirection - as the sole PSU authentication procedure supported by the dedicated interface – will also obstruct the use of TPP-serviced devices such as POS terminals, smart watches or voice automation and hinder further service innovation in this area. Therefore, we propose that the use of redirection is not considered an obstacle to the provision of TPP services only if it is one of multiple customer authentication procedures supported over the dedicated interface.

Overall, we encourage the FCA to consider *feature parity* - between the dedicated TPP interface and all PSU direct access channels deployed by an ASPSP – as a qualifying condition to be met by dedicated interfaces that receive an exemption. TPPs expect that the dedicated interface will deliver such feature parity (on capabilities, availability, user experience and overall performance) to match the PSU direct access channels.

We support the FCA approach to detail the information that is required to support an exemption assessment request; we also support the proposed timeline to review an exemption request (1 calendar month).

**Q2: Do you agree with our proposal to require quarterly submission to us of the quarterly statistics ASPSPs are required to publish under the SCA-RTS? If not, please explain why?**

The EMA supports the FCA proposal that ASPSPs should submit to the FCA the quarterly statistics on the performance and availability of the dedicated interface that they will also be publishing in an accessible location. We invite the FCA to provide more clarity on the latest date of first publication of these interface statistics by ASPSPs. Paragraph 17.109 of the Consultation Paper states that ASPSPs are expected to provide a Plan that identifies the date of first publication of these statistics; however, it is not clear whether the FCA has any expectations as to the date of first public availability of such statistics. Since these statistics will form an important part of the FCA interface monitoring process, it would be useful to detail any FCA expectations on this topic.

**Q3: Do you agree with our approach to receiving reports about problems with dedicated interfaces? If not, please explain why.**

We have some concerns on the proposed process for sending reports of problems with dedicated interfaces to the FCA. Specifically:

1. It is not clear that Card-based payment instrument issuers (CBPIIs) can use the Notification process detailed in paragraph 17.175 (and the Notification Form listed in SUP15 Annex 3D) to report unavailability of the dedicated interface. The *unavailability* definition appears to be limited to PISP/AISP payment account access attempts.

It is not clear how TPPs that use the dedicated interface will be able to report any differences in the level of support they receive in comparison to the PSU direct access interface? TPPs do not have access to any hard data on support levels that an ASPSP extends over different payment account access interfaces. *Note that no such data are included in the published quarterly statistics dataset.*

**Q4: Do you agree with our changes to the Approach Document to reflect the EBA exemption guidelines, EBA Opinion and the SCA-RTS? If not, please explain why.**

The EMA support the core changes introduced in the FCA Approach document to reflect EBA RTS/Guidelines and Opinion documents published in 2018 under the EBA PSD2 mandate. However, we have concerns on the impact of specific document changes; these are detailed below:

1. The text detailing the contingency mechanism (Par. 17.96-17.97) only calls out the ASPSP customer banking portal as the mechanism that TPPs can use to receive payment account access in case of unavailability of the dedicated interface. Does the FCA consider this to be the only appropriate contingency mechanism rather than an ASPSP mobile banking site or native app?

2. The text detailing the contingency mechanism (Par. 17.96-17.97) appears to limit the scope of RTS obligations that the contingency mechanism has to meet to the general obligations for access interfaces detailed in RTS Art. 30. However, a review of the RTS text itself confirms that to achieve compliance with the requirements in RTS Art.30, an interface also needs to comply with RTS Art. 34 (Certificates), Art. 35 (Security of communication session) and Art. 36 (Data Exchanges). Does the FCA propose to defer applicability of these RTS Articles to the contingency mechanism? In the context of the comments above, it is not clear how/why the contingency mechanism differs from the modified customer interface. We would invite the FCA to highlights such differences more clearly.

3. Par 17.136 appears to allow PSUs to carry out direct account selection (to complete an AISP or PISP service transaction) within the ASPSP domain by ASPSPs that allow redirection. The introduction of such functionality should be accompanied by the introduction of a requirement for ASPSPs to pass adequate information on the selected account to the originating AISP or PISP so that they can provide adequate customer service support to their user.

4. Par 17.147 puts forward the FCA view that live eIDAS certificates need not be used by the ASPSP interface testing facility and test interface. Instead, the functionality of such certificates can be "replicated" by the testing facility. Recent payment account access interface deployments (for example by the Open Banking Standard Implementation Entity) have highlighted the interface user authentication/identification framework as a major stumbling block that can delay live service deployments. In this context, the approach adopted by the

FCA increases the risk of authentication framework discrepancies between the test and live dedicated access interfaces.

5. Par. 17.162 advises ASPSPs to have "*…the main interface functionality, which is likely to be subject to the most demand, in use before seeking an exemption*". It is not clear how ASPSPs will be able to identify the most popular access interface functionality in advance of submitting an exemption request. Can ASPSPs really predict whether it will be AISP account access or PISP account access that may be the access functionality that is most requested?

6. Reviewing the text in paragraphs 17.166-17.168, we want to highlight the impact on TPP operations of the activation of the contingency mechanism by an ASPSP (either due to unavailability of the dedicated interface or due to the revocation of an exemption). The user experience of TPP customers will be impacted by this ASPSP action likely resulting in increased numbers of abandoned transactions and confusion among TPP users. TPPs will also be required to implement their own contingency measures to deal with the activation of the contingency mechanism by an ASPSP. We invite the FCA to request that ASPSPs inform all TPPs - that use a dedicated interface - that the contingency mechanism has been activated. We also invite the FCA to monitor actively the compliance of ASPSPs with the text in Par 17.168 ("*Reliance on the contingency mechanism should be a temporary measure*").

7. The text in Par.17.178 does not make it clear whether a PISP can report to the FCA the consistent non-delivery of supporting information to manage payment execution risk over the dedicated interface of an ASPSP. It is likely that some ASPSPs will deliver positive payment transaction confirmation response to a PISP without considering other relevant information (pending/booked transactions, existing overdrafts etc.) leading to subsequent incomplete payment transactions and a poor PISP customer experience. We invite the FCA to provide more clarity on the reporting options available to a PISP in such an interface non-performance scenario.

8. The text in Par.20.18 is missing a reference to the card PAN as a card data field that cannot be used as a knowledge-based authentication factor as detailed in the *EBA Opinion on the implementation of the SCA on SCA and CSC.*[3]

[3] Opinion paragraph 35.

9. The text in Par. 20.19 does not make it clear whether the use of a One-Time Password (OTP) delivered over SMS can deliver confidence that an unauthorized individual has not received (temporary) access to a multi-channel customer device.

10. It is not clear whether the payment account blocking/unblocking functionality detailed in Par 20.30 has to be made available to PSUs of TPP services. We invite the FCA to provide guidance on this subject.

11. The text in Par. 20.31 limits the applicability or RTS Art. 4(3) (d) to an online banking platform; the original RTS text does not include such a limitation and can be interpreted to apply to other access channels.

**Q5: Do you agree with our approach to receiving notifications relating to the fraud rate? If not, please explain why?**

We assess the fraud rate notification requirements detailed in SUP 15.14.29-15.14.34 to be appropriate.

**Q6: Do you agree with our proposed approach to the corporate payment exemption? If not, please explain why.**

The EMA have some concerns on the proposed interpretation of RTS Art.17 (Secure corporate payment processes and protocols) detailed in Paragraphs 20.55-20.69. Specifically:

1. The text in Par 20.56 limits the users of such corporate processes to incorporated entities. This limitation will disrupt the business operations of EMA members that offer access to corporate payment processes to unincorporated entities (e.g. NHS Trusts, partnerships such as solicitors and healthcare providers, corporate cooperatives that offer centralised payment services to SMEs etc.). We want to highlight that these unincorporated entities are not consumers; therefore, they comply with the qualifying condition that appears in Art. 17 of the RTS. We invite the FCA to review this limitation.

2. The text in Par 20.57 is too generic to provide any real guidance on the identification of corporate payment processes. The majority of payment protocols that are currently in use include automated host-to-host processing and the use of access-controlled networks. Additionally, the footnote referenced in this Paragraph includes a reference to "*a dynamic*

*connection between a company and its banking partners*" that is not representative of many existing corporate payment protocols, such as SWIFT.

3. The last sentence of Par 20.60 introduces a requirement for PSPs to demonstrate that payments initiated through the use of corporate payment processes and protocols (that benefit from the relevant SCA exemption) exhibit lower fraud rates than equivalent payment transactions where SCA is applied. However, it is not clear how PSPs that only offer secure corporate payment processes and protocols and do not apply SCA to any processed payment transactions will be able to meet this requirement. We invite the FCA to provide clearer guidance on this topic.

4. It is not clear why dedicated online business banking solutions and physical corporate cards (that incorporate additional company-side administration controls) fail to meet the definition of corporate payment processes/protocols in RTS Art.17.

   We support the FCA approach to assessing the security of corporate payment processes/ protocols through a review of the annual security risk assessment submitted to the FCA.

**Q7: Do you agree with our proposed approach to the application of the strong customer authentication requirements and associated exemptions? If not, please explain why.**

Overall, we support the FCA approach to the application of SCA requirements and SCA exemptions. We invite the FCA to monitor the SCA application practices of ASPSPs for TPP-initiated account interactions after 14 September 2019. A number of EMA members are concerned that ASPSPs will use a blanket approach to apply SCA for most TPP-initiated transactions, thus impacting the user experience of TPP service users. We would welcome FCA guidance to the ASPSP and TPP community on this topic.

**Q8: Do you agree with our approach to implementing the EBA fraud reporting guidelines? If not, please explain why?**

As the FCA has already noted, we are concerned about the increased reporting frequency and the expanded scope of fraud category data introduced in the final version of the *EBA fraud reporting guidelines*. Apart from the data collection in 2019 in order to compare data before and after the RTS on SCA and CSC comes into force, it is not clear why a 6 monthly submission of data is

necessary. Annual reporting appears to be suitable to fulfil the requirements of PSD2 Article 96(6), which requires reporting of data on an annual basis. It is also unclear why the disparity between larger and smaller firms justifies larger firms reporting every 6 months. Each PSP's compliance function will be utilised to run frequent reports every six months rather than focus on fraud prevention efforts.

We also note that the FCA has requested PSPs to submit the first revised fraud report within one month of the end of the 6-month reporting period ending on 31 July 2019; subsequent reports are required to be submitted within 2 months of the end of following reporting periods. We propose that the FCA aligns the final dates for submission of *all* revised fraud reports (including the first one) to *two months* after the end of the preceding reporting period. Here, we want to highlight the additional overhead borne by PSPs that have to switch reporting frequencies/formats from the existing FCA fraud reporting framework to the new framework detailed in SUP 16.13 of the revised Handbook.

The different categories of data that a PSP is required to report on with respect to fraud and complaints are not aligned. This disparity between reporting categories creates unnecessary work for PSPs and imposes a burden on PSPs by way of additional expense and development costs.

Examples of disparity in the categories of fraud data in the fraud and complaints returns are as follows:

- With respect to e-money, the fraud return requires reporting of "*E-money payment transactions with e-money issued by resident PSPs*". However, the complaints return requires reporting to be carried out in respect of "*Issuing or redemption of e-money*" and "*Pre-paid cards and e-money payments*";
- The fraud return focuses on cash withdrawal whereas the complaints return focuses only on ATM withdrawal;
- Where the fraud return divides cards payments in two categories (issued by the resident PSP or acquired by the resident PSP), the complaints return provides '*debit / credit cards*' and '*merchant acquiring*'.

We consider that the fraud and complaints reporting processes would be more efficient - both for the PSPs and the FCA - if the fraud data reporting categories were aligned. First, PSPs would be able to provide reports more swiftly to the FCA if PSPs were able to reuse data they had prepared for a previous report. As PSPs are now required to report every 6 months, reusing previously

prepared data would be a welcomed time saving measure. Secondly, aligning fraud and complaint data reporting categories would allow PSPs to implement common internal reporting software that services multiple types of regulatory reporting, thereby benefiting from implementation and development cost savings.

**Q9: Do you have any feedback on how the FCA can best use the data we would receive under the EBA fraud reporting guidelines?**

The EMA would encourage the FCA to share aggregate/anonymised fraud data with payment industry participants to highlight emerging fraud trends and also allow the industry to assess the effectiveness of SCA methods (and of the SCA exemption framework). This would allow PSPs to gain a greater understanding of the risks facing their industry outside the risks facing their own business. Specifically, a compliance function within a PSP would be able to interrogate the data and identify any blind spots and risks that have not yet threatened their individual business and customers. A compliance function could then implement security measures within their own programme that address these previously unidentified risks. Publishing of fraud data will also give PSPs greater incentive to actively engage in the reporting process rather than treat it purely as compliance exercise.

Additionally, we would encourage the FCA to use the fraud data it receives to further rationalize fraud reporting requirements and eliminate instances of double reporting (of the same fraudulent transaction by multiple PSPs).

Finally, we would encourage the FCA to use its experiences of receiving/processing fraud data with the EBA and other national competent authorities with a view to informing the future revision of the EBA Fraud Reporting Guidelines.

**Q10**: **Do you agree with our proposal to require PSPs and Credit Unions to record and report data on complaints they have received about alleged APP fraud in general? If not, please explain why.**

We agree with the proposal to require PSPs and Credit Unions to record and report data on complaints they have received about alleged APP fraud in general.

However, the EMA would like to highlight the importance of uniformity in the definitions of the terms used, in order to have a coherent regulatory framework and reduce the compliance burden for PSPs.

We note that the proposed Glossary definition for APP fraud – "a transfer of funds…." is inconsistent with the definition set out in the scope of the draft Voluntary Industry Code for a Contingent Reimbursement Model (CRM) i.e. push payments made by consumers through the interbank payment systems:

- push payments executed across CHAPS, Faster Payments
- 'on-us' book transfers where both the sending and receiving accounts are held with the same PSP, and the payment would otherwise have been executed across CHAPS or Faster Payments.

We note that the FCA differentiates APP scam Fraud from "manipulation fraud", which is described in the EBA Guidelines on Fraud Reporting as "*payment transactions made as a result of the payer being manipulated by the fraudster to issue a payment order, or to give the instruction to do so to the payment service provider, in good faith, to a payment account it believes belongs to a legitimate payee ('manipulation of the payer')".*

It is our understanding that 'manipulation fraud' is a subset of APP Scam Fraud, under the FCA's proposed definition. PSPs will therefore be required to report complaints related to the wider group of frauds falling under the definition of "APP Fraud" on an annual basis. They will also be required to report data related to the subset of fraud falling under the definition of "manipulation" on a 6-monthly basis along with all other fraud data reporting required under the EBA Guidelines. We would be grateful if the FCA could confirm this understanding. In many cases it may be difficult for PSPs to differentiate 'manipulation fraud' from 'APP Scam Fraud'.

**Q11: Do you agree with our proposed Approach Document text clarifying our expectations in relation to PSPs' requirements where the wrong unique identifiers are used? If not, please explain why?**

We agree with the FCA's proposed approach.

**Q12: Do you agree with our proposed Approach Document text clarifying guidance in light of the contingent reimbursement code developments? If not, please explain why?**

We propose the following amendment to the text of [8.297] to provide clarity on the status of the proposed CRM.

"*We are generally supportive of work by industry to facilitate the recovery of funds in other cases involving fraud. Industry efforts to develop a 'contingent reimbursement model' (CRM) would see PSPs enter into a voluntary scheme to help to address cases of customer detriment due to APP fraud. Under this scheme, if a PSP* ***failed to meet its duty of care as set out in the Voluntary Code*** ~~*could have taken steps to prevent instances of APP fraud*~~ ***(for example, by*** ~~*such as*~~ *shutting down the accounts of fraudsters, or implementing confirmation of payee), the PSP will help to reimburse the customer. PSPs are under an obligation to comply with legal requirements to deter and detect financial crime as detailed in Chapter 19 – Financial Crime*."

**Q13: Do you agree with our other changes to the Approach Document? If not, please explain why. Please provide section references in your response.**

The EMA welcomes the changes proposed by the FCA to Chapter 3 on Authorisation and Registration. The EMA welcomes in particular, the FCA proposals to provide an alternative contact person to contact if an applicant's assigned case officer is unavailable. We also particularly welcome the FCA's proposal that the designated case officer will give the applicant an update on the current status of their case at least monthly and often more frequently.

**Q14: Do you agree with our proposed changes to PERG regarding agents? If not, please explain why.**

Yes, the changes are consistent with agency arrangements. They will allow unregulated entities to become agents so that they can provide regulated AIS services whilst going through the process of applying for RAISP authorisation themselves.

The changes will support innovation in the payments market, and encourage providers of AIS services to bring new products to market, thus offering consumers more choice and increasing competition. As RAISP agents will be building to the Open Banking technical specifications, the changes to PERG will contribute towards the success of Open Banking.

The regulated entity – the RAISP – must remain responsible for due diligence, compliance monitoring and ongoing audit of the agent, including client agreements and SLAs. The RAISP must also have full oversight of the agent for the duration of the agency agreement.

**Q15: Do you agree with our proposed changes to PERG regarding e-commerce platforms? If not, please explain why.**

Yes the changes are helpful. These are however likely to be a minority of platforms, with the majority acting as e-commerce platforms without undertaking escrow services. Clarification that these can continue to benefit from exclusion when acting for one party only and authorised to negotiate or conclude the transaction would be helpful.

**Q16: Do you agree with our proposed changes to PERG regarding closed loop gift cards? If not, please explain why.**

Yes we concur that where the issuer and payee are the same entity, there is no payment service, rather it is prepayment for goods and services.

**Q17: Do you agree with these changes to PERG? If not, please explain why.**

Overall, the changes are helpful; we do however have some concerns:

Reference at paragraph (c) to monetary value being stored on a specific 'payment' instrument may give rise to confusion. Storage is simply a technical feature, and usually refers to the database or electronic copy of the value that exists on a server or storage device; it is not helpful to qualify it as a 'payment instrument' which has a function. We suggest deleting the word 'payment' and replacing 'instrument' with device.

Alternatively, the PSD2 wording: "services 'based' on specific payment instruments", may also be helpful.

**Q18: Do you agree with the cost and benefits we have identified? If not, please explain why.**

The EMA wish to share the following comments on the Cost Benefit Analysis (CBA) detailed in ***Annex 2*** of the CP. These are:

1. We would challenge the statement in Par.10 of the CBA that states that the revised Approach Document does not introduce new or additional reporting obligations. We would point to the new fraud rate reporting obligations (related to the use of the Transaction Risk Analysis SCA exemption) and the revised statistical fraud rate reporting obligations.

2. The Costs section (in Par. 17 of the CBA) does not appear to consider the costs incurred by the new payment service providers introduced by PSD2 (PISPs, AISPs and CBPIIs) to report dedicated interface problems.

3. It is not clear how the FCA took into account the feedback it has received on the increased costs borne by PSPs to meet the revised statistical fraud reporting requirements (outlined in Par. 33 of the CBA). The costs are exacerbated by the inconsistency of definitions of fraud types between complaints and fraud data reporting requirements.

4. The FCA has concluded that the AISP cost of collecting/reporting the revised fraud data (detailed in SUP 16.13) will be "*minimal*". We invite the FCA to provide more detail on the AISP feedback it considered when coming up with this conclusion. We would suggest that AISP feedback is particularly relevant since this an optional FCA decision that goes beyond the EBA requirements detailed in the *EBA Guidelines on Fraud reporting*.

**List of EMA members as of October 2018:**

Airbnb Inc
Allegro Group
American Express
Azimo Limited
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network Ltd
Boku Inc
CashFlows
Circle
Citadel Commerce UK Ltd
Coinbase
Corner Banca SA
Curve
Ebanx
eBay Sarl
Epayment Systems Ltd
Euronet Worldwide Inc
Facebook Payments International Ltd
First Rate Exchange Services
Flex-e-card
Flywire
GoCardless Ltd
Google Payment Ltd
IDT Financial Services Limited
Imagor SA
Intuit Inc.
Ixaris Systems Ltd
Merpay Ltd.
MuchBetter
Nvayo Limited
One Money Mail Ltd
Optal
Ozan
Park Card Services Limited
Paybase Limited
Payoneer
PayPal Europe Ltd
PayPoint Plc
Paysafe Group
PPRO Financial Ltd
PrePay Solutions
QIX Ltd
R. Raphael & Sons plc
Remitly
SafeCharge UK Limited
Securiclick Limited
Skrill Limited
Starpay Global Ltd.
Stripe
Syspay Ltd
Transact Payments Limited
Transact24 (UK) Ltd
TransferMate Global Payments
TransferWise Ltd
TrueLayer Limited
Trustly Group AB
Uber BV
Valitor
Vitesse PSP Ltd
Viva Payments SA
Wave Crest Holdings Ltd
Wirecard AG
Wirex Limited
Worldpay UK Limited
XCH4NGE LTD