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

To
Amendments to the Money Laundering Regulations 2017 Consultation
Sanctions and Illicit Finance Team
HM Treasury
1 Horse Guards Road
SW1A 2HQ

Anti-MoneyLaunderingBranch@hmtreasury.gov.uk

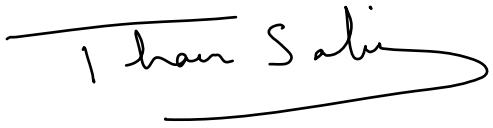
Dear Shantel

Re: Call for Evidence: Review of the UK's AML/CFT regulatory and supervisory regime

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. They also include a growing number of Payment Initiation Service Providers (PISPs). The EMA sits on OBIE's Implementation Entity Steering Group and participates in European initiatives under the aegis of the Euro Retail Payment Board. A list of current EMA members is provided at the end of this document.

We welcome the opportunity to respond to the Call for Evidence. We have not responded to every question in the consultation. I would be grateful for your consideration of our comments and proposals.

Yours sincerely,



Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

EMA Response

1. **What do you agree and disagree with in our approach to assessing effectiveness?**

The government's approach of using FATF methodologies and objectives to establish effectiveness, combined with the findings from the recent FATF review of the UK as a source of evidence, appear to be the most sensible option. The FATF review was thorough and conducted by independent assessors, so would be the best source material for an objective view of the UK AML/CFT framework.

2. **What particular areas, either in industry or supervision, should be focused on for this section?**

No comment.

3. **Are the objectives set out above the correct ones for the MLRs?**

The objectives listed are valid.

We would however suggest that the regulated sector working in partnership with supervisors and the government to improve the collective understanding of ML/TF threat should not be listed as a secondary objective but instead as a primary objective; this activity is a fundamental component in developing the collective understanding of ML/TF risk.

4. **Do you have any evidence of where the current MLRs have contributed or prevented the achievement of these objectives?**

No comment.

High-impact activity

5. **What activity required by the MLRs should be considered high impact?**

Conducting customer due diligence and ongoing monitoring of customers and transactions has a high impact on firms' operations, in particular the verifying of some elements of identity such as address.

6. **What examples can you share of how those high impact activities have contributed to the overarching objectives for the system?**

No comment.

7. **Are there any high impact activities not currently required by the MLRs that should be?**

No comment.

8. **What activity required by the MLRs should be considered low impact and why?**

National Strategic Priorities

9. **Would it improve effectiveness, by helping increase high impact, and reduce low impact, activity if the government published Strategic National Priorities AML/CTF priorities for the AML/CTF system?**

The National Risk Assessment appears sufficient – it is unclear what the added value would be in publishing further Strategic National Priorities.

EMA members would however welcome further input from supervisors regarding strategic supervisory priorities, and the sharing of any areas of concern or key findings from AML/CFT supervisory work. This would assist firms in performing their compliance duties effectively.

10. **What benefits would Strategic National Priorities offer above and beyond the existing National Risk Assessment of ML/TF?**

No comment.

11. **What are the potential risks or downsides respondents see to publishing national priorities? How might firms and supervisors be required to respond to these priorities?**

No comment.

Extent of the regulated sector

12. **What evidence should we consider as we evaluate whether the sectors or subsectors listed above should be considered for inclusion or exclusion from the regulated sector?**

The inherent ML/TF risk presented by AISPs and PISPs is low and for PISPs in particular, consider that their role as intermediaries between payment service users and other financial institutions, reduces the risk of money laundering within the payment chain. Taking each service in turn:

Payment Initiation Services (PIS):
PIS products enable the initiation of transactions from one regulated payment account holding (servicing) payment service provider to another; both of which will be regulated for prudential, conduct, financial crime risks, and will have put in place CDD, monitoring and reporting processes and controls. The PISP is responsible for generating payment orders based on a request from the payment service user (PSU) and does not influence the execution of the payment. The payment order simply represents the PSU's instruction to initiate the payment.

PIS providers do not open payment accounts and cannot hold user funds, nor can the PISP influence the size, frequency or timing of transactions, other than refusing to initiate a transaction entirely. The ML/TF risk is therefore not increased by the use of a PISP as compared to the customer submitting the payment order directly themselves. In some cases, the presence of the PISP in the payment chain may act to reduce ML risk, as the PSU is required to expose their activities to an additional financial institution.

Account Information Services (AIS):
AIS products involve no initiation or execution of payment transactions; AISPs have read-only access to customer bank account information and the AISP cannot conduct any financial transactions on a payment account. AISPs cannot influence any kind of activity

that could give rise to money laundering and are simply independent observers of the activities undertaken by their customers.

It is arguable that without specific consent and authority, AIS providers are not entitled to review their customers' data, which originate elsewhere and to do so would be an abuse of their customers' expectations of trust and confidentiality. Given that all financial services related data will have already been reviewed, and be subject to monitoring and reporting obligations by the relevant account service provider, this emphasises the duplication of effort and further reinforces the absence of a nexus between an AIS service and anti-money laundering risk mitigation objectives.

13. Are there any sectors or sub-sectors not listed above that should be considered for inclusion or exclusion from the regulated sector?

No comment.

14. What are the key factors that should be considered when amending the scope of the regulated sector?

When amending the regulated sector, HMT should take into consideration the inherent ML or TF risk posed by that sector to the UK as a whole, and the likelihood of such products being used to launder funds at large scale.

Innovative payments sectors are often associated with higher AML risk. However in terms of scope and size of market share, they are insignificant in comparison to banks or other sectors such as Estate Agents or High value dealers in relation to money laundering risk.

Enforcement

15. Are the current powers of enforcement provided by the MLRs sufficient? If not, why?

The current powers of enforcement appear to be effective.

16. Is the current application of enforcement powers proportionate to the breaches they are used against? If not, why?

No comment.

17. Is the current application of enforcement powers sufficiently dissuasive? If not, why?

Generally, the application of enforcement powers are largely dissuasive as fines do have a deterrent effect for firms, along with other uses of remediation powers and S166 to build better compliance controls when failings are identified. A central body with oversight of all UK regulators to ensure consistency in approach and use of enforcement powers may be helpful.

18. Are the relatively low number of criminal prosecutions a challenge to an effective enforcement regime? What would the impact of more prosecutions be? What are the barriers to pursuing criminal prosecutions?

Barriers to the risk-based approach

19. What are the principal barriers to relevant persons in pursuing a risk-based approach?

EMA member firms need to have a good understanding of AML/TF risk, and adopt an effective risk-based approach where possible. The barriers to adopting such an approach can arise when their approach is challenged by regulators when it is outside the regulator's experience as it may be different from existing well-known approaches.
Other barriers can arise where technology is used in preference to manual review, for example in transaction monitoring or PEP and Sanctions screening. Often a technological solution can be more effective with correct oversight but may be challenged if it is not the default approach.

20. What activity or reform could HMG undertaken to better facilitate a risk- based approach? Would National Strategic Priorities (discussed above) support this?

Firms would welcome feedback from regulators on the findings from their supervisory work and any common failings they see. This information is crucial to allow firms to ensure their own systems and controls are effective.

21. Are there any elements of the MLRs that ought to be prescriptive?

No.

Understanding of risk

22. Do relevant persons have an adequate understanding of ML/TF risk to pursue a risk-based approach? If not, why?

EMA members need to have a good understanding of risk in terms of ML and TF to be authorised. Where weaknesses have been identified, for example following a sectoral thematic review, sector-specific training can be provided. The EMA has provided such training for members, focusing on areas identified by the FCA as needing improvement. This included the Business Wide Risk Assessment and Customer Risk Assessments.

Firms were already using BWRA templates effectively to monitor risk and apply resources effectively to mitigate the inherent risks.

23. What are the primary barriers to understanding of ML/TF risk?

24. What are the most effective actions that the government can take to improve understanding of ML/TF risk?

Regulators could share best practice around BWRA and CRA based on the results of audits and supervisory work.

Another useful type of information would be case typologies and red flags that are identified by law enforcement and regulators when they investigate ML and TF, which when shared

with firms can be used to identify such activity in their businesses or amongst their customers.

Expectations of supervisors to the risk-based approach

25. **How do supervisors allow for businesses to demonstrate their risk-based approach and take account of the discretion allowed by the MLRs in this regard?**
26. **Do you have examples of supervisory authorities not taking account of the discretion allowed to relevant persons in the MLRs?**
27. **What more could supervisors do to take a more effective risk-based approach to their supervisory work?**

A risk-based approach means that supervisors understand the ML/TF risks, and take the appropriate action to mitigate them. This flexibility allows for a more efficient use of resources, and a dynamic approach to changing threats.

The EBA reported on its findings in February 2020 from reviewing the AML and CFT frameworks of seven competent authorities within the EEA. It was noted that very few member states assessed had an effective risk-based approach where supervisory resources are focused in an aligned way where the highest ML and TF risks exist. It was common theme that competent authorities found it difficult to translate theoretical risk profiles into practical supervisory plans and greater direction in this regard could be useful.

In the report the EBA indicated it was planning to initiate training for competent authorities to improve understanding of risk and effectiveness of supervision measures but it is not clear if this solution will work.

Resources should be focused on obliged entities within each member state that present the highest risk. Supervisory plans should be risk based and focus resources where they are needed most. The type of supervisory engagement should be fitted to the risk rather than to a default position involving an onsite visit in all circumstances.

New and emerging risks should be identified and where supervisors lack knowledge or understanding they should seek fact finding meetings with firms to understand the sectors they are regulating so they can increase their effectiveness. Once the sector becomes better understood any changes that means in practical terms to the UK NRA should be made as soon as possible.

28. **Would it improve effectiveness and outcomes for the government and / or supervisors to publish a definition of AML/CTF compliance programme effectiveness? What would the key elements of such a definition include? Specifically, should it include the provision of high value intelligence to law enforcement as an explicit goal?**
29. **What benefits would a definition of compliance programme effectiveness provide in terms of improved outcomes?**

Expectations from Supervisors on firms would be clearly articulated and therefore understood by firms. Firms can used published compliance objectives to conduct a gap analysis on their own controls and drive improvement and quality in their own frameworks.

Application of enhanced due diligence, simplified due diligence and reliance

30. **Are the requirements for applying enhanced due diligence appropriate and proportionate? If not, why?**

31. **Are the measures required for enhanced due diligence appropriate and sufficient to counter higher risk of ML/TF? If not, why?**

32. **Are the requirements for choosing to apply simplified due diligence appropriate and proportionate? If not, why?**

A risk-based approach for choosing to apply SDD is appropriate, and allows individual firms to make the appropriate decision within the circumstances pertaining to the product, the customer and other risk parameters. We are supportive of this approach and would resist any more restrictive criteria being introduced, that could have the effect of eroding the risk-based approach.
Separately, and in relation to e-money; the continued reduction in exemption limits on E-money cards and wallets are disproportionate, as the risk of ML and TF is minimal for such products, yet value limits have been dramatically reduced. These products can be useful for the financially excluded, or simply as a way to pass on value, such as a gift card. There has been no evidence of systematic abuse of these products, and particularly for the lower limit cards, we believe a higher limit in the region of GBP 500 is appropriate.

33. **Are relevant persons able to apply simplified due diligence where appropriate? If not, why? Can you provide examples?**

The circumstances in which SDD can be used was becoming more and more limited as a result of EU Guidance and SNRA approaches to e-money. We hope that the UK can take a more evidence-based approach an enable e-money products to be used whilst utilising SDD, with fewer restrictions on aggregate turnover or balance limits. These should subjective and driven by the risk assessment relating to the product and the manner in which it is deployed. For some low value products, the cost of full CDD can often outweigh the profit from providing the product at all. Where PEP screening is mandated irrespective of the utility of the product in this context, this also erodes the value of the risk-based approach.

34. **Are the requirements for choosing to utilise reliance appropriate and proportionate? If not, why?**

Reliance as provided for under Regulation 39 is appropriate in a narrow range of circumstances; namely one where a number of regulated entities are involved in a single transaction and are prepared to share such information with one another. They would also be willing to entertain sharing evidence of verification at a later date.

There is a broader need for reliance within an SDD context, where one obligated entity can utilise the CDD undertaken by another entity within low risk parameters, without needing to enter into a contractual agreement with the party being relied upon or seeking documents

from such party. This is not contemplated by the reliance provision but is available to obligated entities within a risk-based framework.

35. Are relevant persons able to utilise reliance where appropriate? If not, what are the principal barriers and what sort of activities or arrangements is this preventing? Can you provide examples?

In practice, the requirement for the party being relied upon to provide documents means that a contractual arrangement between the parties is required, this is very difficult to put in place where relationships are short lived or occasional. Furthermore the concern of parties being relied upon that they may be open to civil litigation in the event that they fail in their CDD duties discourages this practice.

36. Are there any changes to the MLRs which could mitigate derisking behaviours?

Banks' conservative attitude and defensive posture in relation to other PSPs is a result of the perceived compliance cost of monitoring these accounts weighed against the commercial value of the individual relationship. Regulators could provide banks with 'safe harbour letters' stating that, provided appropriate risk based due diligence and ongoing monitoring is implemented, they would not be held responsible for the AML failings of their regulated PSP clients.

Alternatively, HMT can consider allowing banks to hold accounts with Bank of England for safeguarding purposes, removing the customer funds related risk from the commercial banking relationship, and enabling banks to deal with PSPs on a commercial basis.

Another possibility is to mandate that banks provide services to regulated PSPs, given that they are subject to the same regulated environment as the banks themselves, and mostly regulated by the same competent authority. Failure by a number of banks to offer services to a PSP would trigger the regulator's ability to instruct a bank or number of banks to offer banking services. This is the approach adopted in France.

In 2015 in the EMA commented on the draft FATF Guidance for a Risk-Based Approach for MVTS. The Guidance includes a section directed at banks taking on MVTS as customers, and at the supervisors of those banks. The EMA response raised concerns regarding the wording and related supervisory expectations set out in this section, and suggested that banks should not be involved in assessing the CDD systems of MVTS operators beyond establishing their existence, as this would establish another layer of supervision as well as more de-risking of entities in the MVTS sectors. Please find below a number of AML expectations that can exacerbate de-risking:

EMA comments on draft	EMA comments
Section 129 considers "*being a new business without an established operating history*" a higher risk factor to be included in	This automatically creates a barrier for startups and new entrants, as access to a bank account is one of the core requirements for the establishment of a business. This also reduces competition in the market.

the credit institution's analysis.	
Section 132 Section 132 requests banks, when they identify a higher AML/CFT risk, to "review the AML/CFT (group-wide) programmes of the MVTS provider, their internal or external audit and other expert's reports, review the list of agents and their monitoring, management and screening practices. A visit to the place of business and/or informative statements sent to third parties to verify the alignment with operating history, where appropriate, may prove helpful to check the existence and activities of the provider. (...) additional steps or EDD may be necessary."	Please note that a large proportion of MVTS will be considered higher risk from a banks' perspective. Applying the requirements set out in this paragraph to the onboarding process involves considerable resource on the part of the bank. This cost is in many cases considered to be higher than the commercial benefit in taking on this category of client. Given that MVTSs are regulated directly by the competent authority, it seems inappropriate that the bank's CDD processes should include a review of the MVTS compliance policies. This suggests that the regulator's supervision is inadequate, and the bank is in a better position to assess compliance by the MVTS. This is exactly the problem that is causing the de-risking phenomenon which is currently causing disruption, as it suggests to banks that they are not only responsible for their own compliance, but ALSO that of their customers. Regulators must take responsibility for the firms that they regulate, and banks should be able to assume a properly authorised institution has in place adequate AML policies and practices.
Paragraph 134 states: "*Banks should have the ability to flag unusual movements of funds or transactions conducted by MVTS providers for further analysis. They should also have appropriate case management systems so that such funds or transactions are scrutinised in a timely manner and a determination made as to whether they are suspicious*."	There needs to be a clear distinction between the monitoring required of MVTS transactions as a client of the bank, from those of the transactions of the customers of the MVTS. The Bank's responsibility is in relation to whether the MVTS behaves and makes transactions that are consistent with that type of business etc. It is NOT the business of the bank to consider whether a particular transaction undertaken by a client of the MVTS is suspicious. This would be untenable, and would place the bank in a position where they could not fulfil such responsibilities. They would neither have necessary access to client information, nor be in a position to assess the merits of transactions. This is again the kind of obligation that would result in banks concluding that they cannot fulfil their AML obligations in relation to MVTS and lead to the termination of such relationships.
Paragraph 141 states: "*Supervisors could encourage banks to engage with the MVTS sector on the measures that the sector could take*	It is not the role of the banks to supervise or guide MVTS on their AML obligations. They are unlikely to understand the sector as well as the MVTS providers themselves, and the supervisory obligations are distinct. The MVTS is responsible to, and subject to the oversight of the regulator. It is required to set up its own risk management

immediately and in the longer term to meet the banks' risk standards which would enable a continuation or start of the business relationship."	policies and not have these determined by a business supplier – in this case its partner bank. It is no more appropriate for a Bank to set the tome of risk management practices of the MVTS provider than it is of any financial institution to another. The main implication is that the competent authority is outsourcing supervision to the banks; an inappropriate and unworkable obligation. The EMA strongly objects to this wording.
The same issues arise at paragraph 160 which states: "*Banks are not expected to know the clients of the MVTS provider, but to assess the policies and procedures in place by the MVTS providers to comply with AML/CFT requirements*."	The implication is that banks should take a view and decide whether the policies and procedures of MVTS businesses are adequate. This additional layer of supervision is neither welcome by banks nor by MVTS providers. Where does it stop? Should banks review every new iteration of the policies, and if so, should they do this when new legislation is issued? This is an inappropriate and disproportionate requirement.

How the regulations affect the uptake of new technologies

37. **As currently drafted, do you believe that the MLRs in any way inhibit the adoption of new technologies to tackle economic crime? If yes, what regulations do you think need amending and in what way?**

38. **Do you think the MLRs adequately make provision for the safe and effective use of digital identity technology? If not, what regulations need amending and in what way?**

39. **More broadly, and potentially beyond the MLRs, what action do you believe the government and industry should each be taking to widen the adoption of new technologies to tackle economic crime?**

The increasing use of new technologies to enhance AML/CFT compliance in the private sector, such as advanced analytic tools, brings new challenges for supervisors but also could be of great benefit. AML Supervisors need to exercise effective oversight over how these new technologies are used. There are also new technologies available for supervision, in particular transforming supervisory data to sharpen risk assessment, as well as improving the supervision process.

The EMA supports the use of technology to identify and target financial crime particularly in transaction monitoring where it can be used to complement and enhance traditional systems. Having a framework from supervisors in to how new technologies are used and developed would increase take up potentially by obliged entities and encourage member states to adopt the new technology and infrastructure required to make its use more effective.

SARs reporting

40. **Do you think the MLRs support efficient engagement by the regulated sector in the SARs regime, and effective reporting to law enforcement authorities? If no, why?**

Yes, the SARs regime is well known and understood by EMA members. Roles and responsibilities within the MLRs are clear in terms of submission of SARs.

41. **What impact would there be from enhancing the role of supervisors to bring the consideration of SARs and assessment of their quality within the supervisor regime?**

It is the NCA's role to encourage best practice and quality control for SARs that are submitted. They work with particular sectors where they perceive a lower overall number of SARs than expected, and can raise specific issues in terms of quality through ongoing liaison with the EMA and other trade bodies and also directly with firms.

Supervisors already take SARs into account when reviewing firms and assessing their AML/CFT controls; it is unclear what purpose any further enhancement of this in the MLRs would serve.
Requiring the industry to inform their supervisor(s) of the content of SARs could give rise to a dual-reporting obligation, which is not efficient and would require significant operational effort. In addition, firms expect the burden of reporting would not end with the submission of a SAR, but would likely lead to follow-up questions and requests for further data or evidence.

Scrutiny from the regulator may impact the content of SARs, and firms may not disclose details that they would have otherwise provided to the FIU.

42. **If you have concerns about enhancing this role, what limitations and mitigations should be put in place?**

The EMA does not believe this role needs to be enhanced. However it is considered necessary, any inconsistency in approach between the FCA and the NCA should be avoided at all costs. Having two entities reviewing the same thing may cause confusion amongst obliged entities, and will certainly lead to duplication.

43. **What else could be done to improve the quality of SARs submitted by reporters?**

There could be greater use of example SARs to educate and encourage best practice. We would also welcome an overhaul of the SAR online portal, and the submission form to ensure it is fit for purpose and completion is straightforward. Use of webinars and other training tools by the UKFIU to drive common standards in all sectors to ensure quality is maintained is also welcomed.

44. **Should the provision of high value intelligence to law enforcement be made an explicit objective of the regulatory regime and a requirement on firms that they are supervised against? If so, how might this be done in practice?**

The term ‘high value intelligence’ may mean something different to firms than it does to supervisors. Firms submit SARs to comply with legal obligations where the requisite suspicion under POCA is established, and are therefore obliged to do so regardless of the value involved or the likely usefulness to the authorities in the submission. It would wrong to penalize firms if they act fully in accordance with law but the SARs they submit prove not be ‘high value intelligence’ in the view of supervisory authorities.

45. **To what extent should supervisors effectively monitor their supervised populations on an on-going basis for meeting the requirements for continued participation in the profession?**

Gatekeeping tests

46. **Is it effective to have both Regulation 26 and Regulation 58 in place to support supervisors in their gatekeeper function, or would a single test support more effective gatekeeping?**

47. **Are the current requirements for information an effective basis from which to draw gatekeeper judgment, or should different or additional requirements, for all or some sectors, be considered?**

48. **Do the current obligations and powers, for supervisors, and the current set of penalties for non-compliance support an effective gatekeeping system? If no, why?**

Guidance

49. **In your view does the current guidance regime support relevant persons in meeting their obligations under the MLRs? If not, why?**

Yes, in particular the JMLSG Sectoral Guidance for E-money is very useful.

50. **What barriers are there to guidance being an effective tool for relevant persons?**

51. **What alternatives or ideas would you suggest to improve the guidance drafting and approval processes?**

Structure of the supervisory regime

52. **What are the strengths and weaknesses of the UK supervisory regime, in particular those offered by the structure of statutory and professional body supervisors?**

Strengths: Good FATF evaluation of UK shows current approach largely effective

Weaknesses: Supervision of AML/CFT at national level is becoming less and less effective in dealing with the cross-border
nature of the financial sector, and in providing a robust AML/CFT framework

53. **Are there any sectors or business areas which are subject to lower standards of supervision for equivalent risk?**

Entities subject to dual regulation by the FCA and HMRC, who have different approaches and expectations may cause uncertainty for firms on how they should best show ML/CFT effectiveness.

54. Which of the models highlighted, including maintaining the status quo, should the UK consider or discount?

55. What in your view would be the arguments for and against the consolidation of supervision into fewer supervisor bodies? What factors should be considered in analysing the optimum number of bodies?

Effectiveness of OPBAS

56. What are the key factors that should be considered in assessing the extent to which OPBAS has met its objective of ensuring consistently high standards of AML supervision by the PBSs?

No comment.

57. What are the key factors that should be considered in assessing the extent to which OPBAS has met its objective of facilitating collaboration and information and intelligence sharing?

No comment.

Remit of OPBAS

58. What if any further powers would assist OPBAS in meeting its objectives?

59. Would extending OPBAS's remit to include driving consistency across the boundary between PBSs and statutory supervisors (in addition to between PBSs) be proportionate or beneficial to the supervisory regime?

Supervisory gaps

60. Are you aware of specific types of businesses who may offer regulated services under the MLRs that do not have a designated supervisor?

61. Would the legal sector benefit from a 'default supervisor', in the same way HMRC acts as the default supervisor for the accountancy sector?

62. How should the government best ensure businesses cannot conduct regulated activity without supervision?

List of EMA members as of October 2021

AAVE LIMITED
Account Technologies
Airbnb Inc
Airwallex (UK) Limited
Allegro Group
American Express
ArcaPay Ltd
Azimo Limited
Bitpanda Payments GmbH
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network Ltd
Boku Inc
CashFlows
Circle
Citadel Commerce UK Ltd
Contis
Corner Banca SA
Crosscard S.A.
Crypto.com
Curve
eBay Sarl
ECOMMPAY Limited
Em@ney Plc
emerchantpay Group Ltd
ePayments Systems Limited
Euronet Worldwide Inc
Facebook Payments International Ltd
Financial House Limited
First Rate Exchange Services
FIS
Flex-e-card
Flywire
Gemini
Globepay Limited
GoCardless Ltd
Google Payment Ltd
HUBUC
IDT Financial Services Limited
Imagor SA
Ixaris Systems Ltd
Modulr FS Europe Limited
MONAVATE
Moneyhub Financial Technology Ltd
Moorwand
MuchBetter
myPOS Europe Limited
OFX
OKTO
One Money Mail Ltd
OpenPayd
Own.Solutions
Oxygen
Park Card Services Limited
Paydoo Payments UAB
Paymentsense Limited
Payoneer
PayPal Europe Ltd
Paysafe Group
Plaid
PPRO Financial Ltd
PPS
Remitly
Revolut
SafeCharge UK Limited
Securiclick Limited
Skrill Limited
Snowy Pay Ltd.
Soldo Financial Services Ireland DAC
Square
Stripe
SumUp Limited
Syspay Ltd
Transact Payments Limited
TransferMate Global Payments
TrueLayer Limited
Trustly Group AB
Uber BV
Vitesse PSP Ltd
Viva Payments SA
Vivid Money Limited
Weavr Limited
WEX Europe UK Limited
Wirex Limited
Wise
WorldFirst
WorldRemit LTD