Prepaid International Forum Ltd, 161-165 Farringdon Road, London, EC1R 3AL
info@prepaidforum.org

Consultation on the Transposition of 5MLD
Sanctions and Illicit Finance Team (2/27)
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ

10 June 2019

Dear Sir or Madam

Consultation on the Transposition of the Fifth Money Laundering Directive

We are writing in response to the consultation initiated by HM Treasury in its document: "Consultation on the transposition of the Fifth Money Laundering Directive" ("5MLD") (April 2019) (the "**Consultation**").

PIF

PIF is the not-for-profit trade association representing organisations who are regulated under electronic money ("e-money") and payment services regulations and who operate in the prepaid and fintech sectors. It is in this capacity that we submit our response to the consultation.

Consultation

We fully support the regulatory goal to combat the use of e- money products and services for unlawful purposes as well as the evidence-driven, risk-based approach to the prevention of financial crime in 5MLD. The rules on the prevention of money laundering and terrorist financing must always ensure that prepaid and e-money products are safe and not abused for the purposes of illegal activities.

PIF strongly believes that in transposing 5MLD the government should take into consideration the range of e-money products available, the benefits they offer and the different customers that they are designed for. We would advocate that the requirements under 5MLD are proportionate to the risks related to these products and do not establish overly burdensome obligations on providers of these products. Therefore, we welcome that the government is inclined to transpose 5MLD as is, maintaining where possible the capacity to provide exemptions.

We have provided our answers to the consultation questions in **Appendix 2** to this letter. We have also provided some general comments on the e-money sector for context and these are set out in **Appendix 1**.

We should add that the views set out herein are those of PIF and do not necessarily reflect the views of all of our members.

If you would like to discuss this response with us, we would be pleased to do so. Please contact Diane Brocklebank in the first instance at diane.brocklebank@prepaidforum.org or on 07736 971 986.

Yours faithfully

On behalf of:
Prepaid International Forum Ltd (PIF)

Encs.

Appendix 1

General Comments on e-money, prepaid and customer due diligence

There is a very broad and growing range of regulated e-money products in the prepaid market. These include gift cards (typically non-reloadable), reloadable prepaid products that are used by consumers and businesses as well as e-money wallets operated through online or mobile based platforms.

Some e-money products are for use by consumers and others are designed exclusively for businesses. Regulated prepaid and e-money products can be used and tailored for a variety of different purposes, such as travel money, gift, as an alternative to a traditional bank account, budgeting and encouraging good money management skills in the student and youth market, as well as corporate products designed for specific corporate or public sector needs. For example, corporate incentives and rewards, expense management, payroll and benefits disbursement.

The type of functionality offered by these products varies accordingly. For example, there may be limitations on who can load value onto the products, whether re-loading is even possible, the means of loading (e.g. credit transfer from an existing UK bank account, loading using a credit or debit card or cash loading), and where the e-money can be spent (e.g. for point-of-sale (POS) transactions and/or card-not-present transactions (e.g. online)) at a selected group of merchants or a large variety of merchants. These products can also enable (but not always do) cash access, i.e. ATM use. The inherent risks associated with the different types of e-money products and their user base vary accordingly.

Regulated firms take these and many other factors into account when applying a risk-based approach to the operation of products which are then restricted, set up, controlled and monitored taking account of the specific product and customer risk profile. Simplified due diligence ("SDD") measures are similarly carefully defined on this basis.

It very is important for regulated firms in our sector to be able to responsibly balance robust anti-money laundering ("AML") controls with product operation that is aligned with the desired user experience and customer use cases. This balance can only be achieved, particularly in the case of innovative payment products and services, if regulated firms are able to apply a risk-based approach.

Appendix 2

Chapter 3: Electronic Money

Question 37: Should the government apply the CDD exemptions in 5MLD for electronic money (e-money)?

Yes, we believe that in order to be able to continue providing innovative and competitive products that provide benefits to consumers, including those who are most vulnerable, the e-money sector has to be able to rely on the CDD exemptions in 5MLD. We therefore welcome the government's expressed intent to transpose 5MLD as is, maintaining the capacity to provide exemptions. In doing so, the Government is taking into consideration the variety and diversity of low-value, low-risk e-money products that currently rely on the CDD exemption.

The CDD exemption was initially introduced to allow easy access to low-value, low-risk e-money products. Consumers often use these types of products for small online spends that guarantee a high-level of security and privacy and that allows the customers to be in full control of their costs.

The restrictive conditions set out in Article 12 4MLD already limit the application of the exemption to low-value e-money payments with limited functionality prepaid products. The attractiveness of such exempt products to criminals and the money laundering and terrorist financing risk they pose is significantly reduced.

If the e-money CDD exemptions are not applied, we are concerned that this will have a negative impact on providers of low-value, low-risk e-money products and services and harm consumer choice of alternative payment products.

Without the ability to rely on e-money CDD exemptions, the cost of undertaking CDD at the outset would be prohibitive for many businesses. The CDD exemption allows customer due diligence to be postponed until the customer has used the product to an extent that justifies undertaking due diligence, both from the perspective of risk and the cost of undertaking CDD. From a consumer perspective, asking customers using low-value products to identify themselves would create unnecessary hurdles and potential barriers to financial inclusion. In a case where an issuer utilises the CDD exemption, it would in many cases still have oversight over the lifecycle of such a product due to transaction monitoring measures that enable the issuer to trace transactions and apply appropriate risk mitigation measures.

We therefore support the application of the thresholds as amended by 5MLD and encourage the government to transpose the CDD exemptions in 5MLD without any changes.

Question 38: Should e-money products which do not meet the criteria for the CDD exemptions in Article 12 4MLD as amended be considered for SDD under Article 15?

Yes, these are mutually exclusive provisions. Accordingly, we support allowing some products which do not meet the criteria for an exemption from CDD under Article 12 to benefit from SDD under Article 15 where, taking into account the product, customer, delivery channel and geographical factors (i.e. the criteria to apply SDD set out in the Directive), the risk is low.

If – pursuant to a risk-based approach – the e-money issuer is satisfied that the risk of money laundering and terrorist financing is low, and the product continues to represent a low risk by ongoing monitoring of both the entity and the transactions, the issuer should be allowed to apply SDD measures in respect of e-money products.

Question 39: Should the government exclude any e-money products from both the CDD exemptions in Article 12, and from eligibility for SDD in Article 15?

No. We believe that general/blanket exclusions would wholly contradict the principle of a risk-based approach enshrined in both 4MLD and 5MLD. We would like to stress that all issuers of e-money products are subject to a requirement to consider and assess the risks of money laundering and terrorist financing by taking into consideration appropriate risk factors in deciding the level of due diligence measures to be undertaken in respect of the products they offer.

Furthermore, both the Article 12 CDD exemption and the Article 15 SDD provisions require firms to carry out transaction monitoring and to have appropriate controls in place in order to identify suspicious transactions.

With appropriate safeguards and risk mitigating factors in place, the money laundering and terrorist financing risk of any product can be lowered and therefore potentially justify the application of SDD measures. In respect of the Article 12 CDD exemption, the conditions imposed on the maximum value and functionality for the e-money product to be considered eligible for the exemption means that the risk posed by these products is already low.

Given the above, we see no reason why any e-money product should be excluded. We believe that to do so would be unreasonable and hinder competition in UK financial services in light of the fact that comparable non e-money products would not be subject to an express prohibition from eligibility for SDD under Article 15 of 5MLD.

Question 40: Please provide credible, cogent and open-source evidence of the risk posed by electronic money products, the efficacy of current monitoring systems to deal with risk and any other evidence demonstrating either high or low risk.

Invariably (and similar to other financial products), the risk posed by e-money products varies with the functionality they offer, such as the type and legal status of the customer the product is targeted at and geographical factors.

However, we would like to stress that regulated e-money products pose no greater inherent risk than any other type of financial services product. For example, e-money products such as an open-loop prepaid card are analogous to credit and debit cards in terms of the risks they pose. All are susceptible to account takeover and there is little to differentiate between card types online.

For example, all Electronic Money Institutions ("EMIs"), as obliged entities under the Money Laundering Regulations ("MLRs"), undertake a financial crime risk assessment. Key measures are subsequently undertaken to allow the firm to mitigate inherent risk and define the relevant controls to combat money laundering and terrorist financing activity. E-money products have a relatively narrow scope of "expected behaviour" due to the fact that it is mostly serving a specific need of a customer, unlike many traditional financial products such as a bank account used for a large variety of customer needs. Transaction monitoring compares actual behaviour to expected behaviour and any deviations are flagged and investigated.

Furthermore, some prepaid products have a distinct advantage over products provided by traditional financial institutions. The advantages being the ability of providers to modify products to reflect certain use cases. For example, there are restrictions on the maximum amount of funds permitted to be stored on prepaid cards making their use much less attractive to criminals. The industry in which our members operate invests heavily in the creation and continual improvement of transaction monitoring systems to prevent their e-money products being used for unlawful purposes, with vast sums of money invested in people, data and technology (such as AI, predictive modelling and machine learning).

For example, for non-reloadable SDD e-money products, many issuers' transaction monitoring systems allow them to link multiple transactions to a device. By blocking these devices which are linked to suspicious usage patterns as well as transactions displaying suspicious usage patterns, issuers can mitigate the risk of these products being used for illegal activity. It is important to note that these risk mitigating measures can be effectively applied without identifying the customer.

Reloadable SDD e-money products offer enhanced possibilities for monitoring user behaviour as they are typically used over a longer period of time and for a larger number of transactions. This enables issuers of these products to gather comprehensive usage data – such as place of loading, place of spend, IP addresses and devices used to initiate payments – that can be reliably traced back to a single individual.

Prepaid card issuers can also set volume parameters on the amount and value of transactions carried out on their e-money products. This again reduces the risk of these products being used for unlawful purposes and triggers alerts to potentially suspicious activity. Furthermore, the amount of times a card can be loaded, and the maximum permitted in a single load can also be specified and controlled by imposing thresholds.

We would also like to point out that certain types of prepaid card programmes – in particular, cards used for corporate expense management – can be modified to restrict the spend at merchants falling within certain merchant category codes ("MCCs"). This can be highly effective at reducing fraud rates for example because with corporate customers the intended card use is specified at the customer on-boarding and risk assessment stage. If a transaction type is deemed not allowed, the corporate could block the facility altogether. For example, where the card is used for online money transfers or to withdraw cash at an ATM.

This offers evidence that prepaid card providers are effectively able to lower the risk associated with certain fraudulent transactions due to their ability to impose restrictions, which may not be possible for debit and credit cards provided by traditional financial institutions.

There is also evidence to suggest that a culture of financial crime prevention is well established in the e-money sector. In October 2018, the Financial Conduct Authority (FCA) published the findings of its thematic review (TR18/3)[1] into money laundering and terrorist financing risk in the e-money sector. The FCA's assessment, which was focused on e-money including prepaid cards and digital wallets, examined the anti-money laundering and counter terrorist financing control frameworks e-money firms have in place. The FCA found that the majority of e-money firms they visited had effective systems and controls in place to mitigate the risks and that most firms had relatively few high-risk customers. The FCA also found that at most firms, transaction monitoring was effective and largely based on automated technological solutions.

It is also important to note that the e-money sector is subject to monitoring systems that are comparable to banking practices, for example transaction alerts and exception reporting as well as picking up on suspicious transaction patterns. Firms in the e-money sector also utilise system-based rules aimed at spotting behaviour which reflect money laundering and terrorist financing typologies which are further investigated by experienced staff. In many instances, firms in the e-money sector are utilising a combination of technologies that are only just starting to be used by financial institutions in the banking sector.

As the prepaid and e-money sectors have grown, the provision of 'RegTech' has grown alongside. For example, our own research[2] into the technologies and procedures firms in the prepaid and fintech sector use to onboard new customers found that firms are rapidly expanding the range of identity verification technologies they use. This allows providers of e-money products to gain a much wider view of a customers' identity either at the point of account opening or ongoing monitoring. Our research also found that firms in the e-money sector routinely go above and beyond regulatory requirements to ensure compliance with their obligations. For example, 57% of firms we surveyed are using new technologies that allow them to examine an applicant's digital footprint and social media accounts to gain further confidence in their identity. Increasingly, providers are looking at newer solutions that provide fraud and client monitoring using AI and Machine Learning techniques.

[1] https://www.fca.org.uk/publications/thematic-reviews/tr18-3-money-laundering-and-terrorist-financing-risks-e-money-sector

[2] https://prepaidforum.org/criminals-and-terrorists-on-the-back-foot-thanks-to-innovative-customer-identity-checks-on-e-money-prepaid-and-fintech-financial-services/

It is fair to say that the size of an e-money firm will dictate its ability to invest in more effective learning technology due to the cost of these systems outweighing the level of losses incurred. However, many systems can and are being utilised cost-effectively, provided the rule sets are modified to accurately reflect an individual e-money firm's risk appetite.

We should also add that firms in the e-money sector have long worked with each other to identify technologies and share information on threats detected where possible. They also engage with law enforcement agencies and are informed by the output of national and international bodies such as the FATF and FIUs.

Finally, it is important to take into consideration that the e-money sector is highly regulated under e-money and payment services legislation. The introduction of Strong Customer Authentication under the Second Payment Services Directive (PSD2) and initiatives such as Confirmation of Payee will reduce the risks posed by e-money products even further.

Question 41: What kind of changes, if any, will financial institutions and credit institutions have to implement in order to detect whether anonymous card issuers located in non-EU equivalent states are subject to requirements in their national legislation which have an equivalent effect to the MLRs?

We acknowledge that the co-legislators intended to prevent anonymous prepaid cards without adequate limits or controls from being brought into the EU. Whilst we entirely share and support the goal of the new paragraph 12(3), we have serious concerns regarding the practical feasibility of implementing the requirements. It will be extremely difficult for acquirers to have sole responsibility for ensuring that anonymous card issuers located in non-EU equivalent states are subject to requirements in their national legislation which have an equivalent effect to the MLRs. We believe that the e-money sector (not just acquirers but all participants in the ecosystem including card schemes) will have to carry out extensive work to understand whether legislation in non-EU states is equivalent to the MLRs in EU member states. This will need to be done both before the changes take effect and on an ongoing basis to ensure compliance in view of any further legislative developments or changes.

It will be necessary for acquirers and for monitoring systems to be able to identify from the Bank Identification Number (BIN) on the card the location of issue. This is already in place for major financial institutions, but this is unlikely to be the case for smaller firms in the e-money sector. It is therefore likely that some firms will need to apply rules configured to detect such cards and have the technology to decline and/or block the use of cards issued by non-EU states which do not comply with the requirements.

Question 42: Should the government allow payments to be carried out in the UK using anonymous prepaid cards? If not, how should anonymous prepaid cards be defined?

We believe the government should allow payments to be carried out in the UK using anonymous prepaid cards. To remove anonymous prepaid cards or restrict the regulatory model of SDD would have negative implications for the UK. For example, it would have far-reaching consequences for vulnerable consumer groups – such as the financially excluded – who rely on these types of cards.

The argument that e-money poses money laundering and terrorist financing risks "because of the anonymity they offer" seems to be based on an assumption that anonymous prepaid cards are completely anonymous and allow for the movement of money without any traceability. This perception is untrue given that all prepaid cards leave an electronic footprint which allows transactions to be traced. Consideration also needs to be given to the fact that all issuers of e-money – including those who issue SDD e-money products – are required to monitor those transactions for any suspicious or unusual activity under the MLRs 2017.

Payments using anonymous prepaid cards are far more traceable than cash even in cases where the customer is not fully identified (see also our answer to question 40). This is due to the availability of detailed transaction records such as time stamps, merchant details and information about where and when the prepaid card was originally purchased. These monitoring data enable transactions to be linked with footage from other sources such as ISPs and security cameras allowing law enforcement agencies to gather evidence to identify and prosecute individuals who use these types of cards for unlawful purposes. We are concerned that any restrictions on the use of anonymous prepaid cards will prompt legitimate users and criminals alike to switch to cash which will only exacerbate the problem associated with anonymity of payments.

The prepaid sector is spearheading the development of payment products that are making financial services accessible, secure and flexible for all parts of society. Low value anonymous prepaid cards are particularly valuable to vulnerable members of society who may lack the identity documents required to access other, sometimes more costly financial products that require full identity verification. Many people still lack regular internet access making solutions such as online activation difficult. If the government prohibits payments to be carried out using anonymous prepaid cards it could force those who rely on these products to make a choice between reverting to cash or losing more of their income to fees which in turn could prompt them to turn to high cost credit.

Many people are attracted to prepaid cards because they offer security and convenience. But they are easily deterred by the requirement to undergo identity verification if they simply want to assess whether a prepaid card will meet their needs. Removing the ability of customers to trial prepaid financial services with a low value anonymous prepaid card will likely have a material impact on the industry and detrimental effect on consumer choice.

We should also point out that where anonymous prepaid cards are used for the purpose of company expenses or incentive payments, the entity and source of funds will have been fully verified.

The government should also note that the vast majority of anonymous prepaid card activity in the UK is represented by the gift card product group. Requiring a formal verification of identity for low-value prepaid cards such as regulated multi-store gift cards would not prove financially viable, leading to a

significant disengagement of e-money issuers from the gift card market. This market is comprised of largely low-value, single load products and they cannot be used to withdraw cash.

Anonymous prepaid cards can be used for unlawful purposes as can cash and any other financial product. But it is important to be realistic about the extent of the risk anonymous prepaid cards pose and balance this against the risk of doing irreparable damage to an innovative sector that is used by millions of law-abiding consumers and businesses every day.

Chapter 4: Customer Due Diligence

Electronic Identification Processes

Question 44: Is there a need for additional clarification in the regulations as to what constitutes "secure" electronic identification processes, or can additional details be set out in guidance?

We would welcome additional details in the guidance that explains how standards can be achieved.

We would particularly like the guidance to address the provision of solutions for vulnerable members of society and those with disabilities for whom processes may cause difficulties or subject them to an increased risk.

Question 45: Do you agree that standards on an electronic identification process set out in Treasury-approved guidance would constitute implicit recognition, approval or acceptance by a national competent authority?

Yes. However, we would welcome confirmation that the standards on electronic identification as set out in Treasury-approved guidance such as JMLSG constitute an implicit recognition of those standards by the UK national competent authority in the guidance itself.

Question 46: Is this change likely to encourage firms to make more use of electronic means of identification? If so, is this likely to lead to savings for financial institutions when compared to traditional customer onboarding? Are there any additional measures government could introduce to further encourage the use of electronic means of identification?

Provided the overarching objective is to mitigate risk, improve efficiency and reduce overall costs, then we believe the changes will encourage firms to make more use of electronic processes in order to maintain business levels on programmes which would otherwise be potentially lost. For smaller firms, the cost of implementation and ongoing use would need to prove to be commercially viable.

If firms already use such technology for other programmes, or if systems are introduced to reduce the number of manual documents, this is likely to encourage the use of electronic means.

Overall, a regulatory environment that promotes the use of modern and secure remote identification methods can lead to savings for financial institutions and their customers. It will also lead to more security and convenience for consumers. Most larger financial institutions already deploy electronic means of identification as many customers also expect financial institutions to offer the possibility of such non-face-to-face means of identification.

We would welcome incentives such as grants to smaller firms or firms whose entire business model has previously been in the production of directly affected programmes to further encourage the use of electronic verification.

Changes to Regulation 28

(Identifying and verifying senior management of a body corporate and measures to understand the beneficial ownership structure)

Question 47: To what extend would removing 'reasonable measures' from regulation 28(3)(b) and (4)(c) be a substantial change? If so, would it create any risks or have significant unintended consequences?

Requiring to verify the names of the full names of the board of directors and the senior persons responsible for the operations of the body corporate (regulation 28(3)(b)) and the identity of the beneficial owners (regulation 28(4)(c), rather than taking 'reasonable measures' to do so could add significant administrative burden, costs and potentially prevent providing services to some corporate customers.

Depending on the corporate structure and the nationality/residence of the directors, senior managers or beneficial owners, the means and methods for independent verification of the names/identities of these persons could be challenging, limited and/or expensive. The change is therefore likely to result in increased costs, both in terms of undertaking extra checks in order to attempt to verify the identities of the beneficial owners and directors and costs of turning away corporate customers where this cannot be achieved.

Question 48: Do you have any views on extending CDD requirements to verify the identity of senior managing officials when the customer is a body corporate and the beneficial owner cannot be identified? What would be the impact of this additional requirement?

We do not believe there would be a significant impact to require to verify the identity of senior managing officials where the customer is a body corporate and the beneficial owner cannot be identified. In such situations, additional checks would be carried out on a beneficial owners regardless. However, there may be implications if the company concerned needs to carry out further research in

order to provide the required level of detail which may result in a slightly longer customer on-boarding time.

Question 49: Do related ML/TF risks justify introducing an explicit CDD requirement for relevant persons to understand the ownership and control structure of customers? To what extent do you already gather this information as part of CDD obligations?

Yes, we believe an explicit requirement for firms to understand the ownership and control structure of their customers is justified. It is important to understand potential clients' company structure ownership and control, especially in cases where the structure is less than straightforward. Only by fully understanding this can providers of e-money products successfully determine the extent of risks involved. Our members routinely adopt this practice as part of their customer on-boarding process.