HM Treasury

Home Office

Date: 11th Nov 2019

Request for Information
National Risk Assessment on Money Laundering and Terrorist Financing

The Home Office and HM Treasury (HMT) are updating the UK's National Risk Assessment on Money Laundering and Terrorist Financing (NRA), to be completed by July 2020 in accordance with the timetable set out in the Economic Crime Plan published in July this year.

As you know, we published the first NRA in 2015, and the second in 2017. The Financial Action Taskforce (FATF) Mutual Evaluation in 2018 found that the UK has a robust understanding of its money laundering (ML) and terrorist financing (TF) risks, which is reflected in our public NRAs; and that our national anti-money laundering (AML) counter-terrorist financing (CTF) policies, strategies and activities seek to address the risks identified in the NRAs. To continue to meet FATF's requirements and standards, and maintain a well-functioning regime, we must continue to update our understanding of where our ML/TF risks lie.

The NRA is dependent on evidence, assessments and case studies from across government, law enforcement, supervisors and the private sector. Information from the private sector informs our understanding of the risks in each sector, and improves the effectiveness of compliance activity.

We are seeking your input through the below questionnaire. Wherever possible, please provide supporting data, statistics and case studies to support your points. We cannot use anecdotal information. Please state if you cannot answer a question due to lack of information. Please provide information from the 1st Aug 2017 to current day.

All information you provide to us will be treated confidentially; if we use any of the statistics or case studies you provide in the published NRA, they will be anonymised. If your data or information is operationally or commercially sensitive, we can discuss alternative means of information sharing such as a form of words, to ensure the protection of sources.

If you are a trade association, you are welcome to distribute this to your members to seek views, but please only provide us with one consolidated response from your organisation and members.

Please complete the below questions in relation to your relevant sectors and send your responses to Rose van der Zwart at Rose.vanderZwart@hmtreasury.gov.uk and Adam David at Adam.David@hmtreasury.gov.uk by **25th Nov 2019**. If you have any questions, please do contact us before the deadline.

Sectors:

- The banking sector
- Financial technologies
- Accountancy services
- Legal services

- Property & estate agency services
- Trusts & corporate structures
- Cash
- Money service businesses
- Non-profit organisations
- Gambling
- High value dealers

Thank you for your assistance.

Kind regards,

Rose van der Zwart
Sanctions and Illicit Finance, NRA Lead
HM Treasury
Rose.vanderzwart@hmtreasury.gov.uk

Stephanie Ukpelukpe
Economic Crime Unit, NRA Lead
Home Office
Stephanie.Ukpelukpe@homeoffice.gov.uk

Organisation: Electronic Money Association

Please briefly outline the services your organisation provides: We are a trade body in the Payments sector and support our members AML and CTF compliance activities.

Would your organisation be interested in participating in a follow-up workshop? Yes, we would be interested.

Question	Your Response (no word limit, expand as required in all sections)
1. What do you believe to be the ML and TF risks in the products and services you offer? *For each, please explain why you think this is a risk.*	The risk factors the EMA understands to be indicative within the E-Money sector are in line with those highlighted in the European Banking Authority Guidelines (JC 2017 37 Final draft Risk Factors AML GL) as follows: <u>Product risk factors:</u> • **Thresholds**: the product allows i.high-value or unlimited-value payments, loading or redemption, including cash withdrawal; ii.high-value payments, loading or redemption, including cash withdrawal; iii.high or unlimited amount of funds to be stored on the e-money product/account. • **Funding method**: the product can be i. loaded anonymously, for example with cash, anonymous e-money or e-money products that benefit from the exemption in Article 12 of Directive (EU) 2015/849; ii. funded with payments from unidentified third parties; iii. funded with other e-money products. • **Utility and negotiability**: the product i. allows person-to-person transfers; ii. is accepted as a means of payment by a large number of merchants or points of sale; iii. is designed specifically to be accepted as a means of payment by merchants dealing in goods and services associated with a high risk of financial crime, for example online gambling; iv. can be used in cross-border transactions or in different jurisdictions; v. is designed to be used by persons other than the customer, for example certain partner card products (but not low-value gift cards); vi. allows high-value cash withdrawals.

	The EMA has produced a table (**Annexe 1 - attached**) covering the types of E-Money products being offered by its membership and their functionality with mitigation details which may have an impact on residual risk within the sector. From the analysis conducted by the EMA we can conclude that E-Money general pre-paid cards and wallets with multiple functions particularly that allow cross border and peer-to-peer (P2P) transactions may pose a greater risk from a ML and TF perspective. However, this is in terms of inherent risk before mitigation measures have been implemented, and the residual risk will depend on the effectiveness of compliance measures deployed within individual firms. <u>Customer risk factors:</u> The following factors may contribute to increasing risk: • The customer purchases several e-money products from the same issuer, frequently reloads the product or make several cash withdrawals in a short period of time and without an economic rationale; where distributors (or agents acting as distributors) are obliged entities themselves, this also applies to e-money products from different issuers purchased from the same distributor. • The customer's transactions are always just below any value/transaction limits. • The product appears to be used by several people whose identity is not known to the issuer (e.g. the product is used from several IP addresses at the same time). • There are frequent changes in the customer's identification data, such as home address or IP address, or linked bank accounts. • The product is not used for the purpose it was designed for, for example it is used overseas when it was designed as a shopping centre gift card. In terms of customer risk, the EMA has identified typologies where accounts may be controlled from several IP addresses and also those where the customer frequently changes his or her identification data. In such circumstances the firm will generally conduct an investigation and seek a rationale from the customer and where this information from the customer does not mitigate the suspicion, a SAR may be generated, and/or the relationship suspend and ultimately terminated. <u>Distribution channel risk factors:</u> • Online and non-face to face distribution without adequate safeguards in terms of know your customer (KYC) verification and customer due diligence (CDD)

	• Distribution through intermediaries – where the E-Money Issuer (EMI): i. relies on the intermediary to carry out some of the AML/CFT obligations of the EMI, and ii. has not satisfied itself that the intermediary has adequate AML/CFT systems and controls • Segmentation of services, in provision of E-Money services by several operationally independent service providers without due oversight and co-ordination In terms of distribution channel risk, where AML oversight may be limited where distributors market products, on behalf an EMI, EMIs mitigate most risks by undertaking compliance processes such as CDD and monitoring centrally, and only relying on the distributor for non-compliance related functions. The use of technology and audits to monitor the activity of a distributor further mitigates such risks. Obviously, where there is a lack of a robust audit and monitoring of outsourced services, the risk can be more significant. The EMA has limited evidence within member firms that outsourced controls are being ineffectively managed and oversight is lacking. <u>Country or geographical risk factors:</u> The following factors may contribute to increasing risk: • The payee is located in, or the product receives funds from sources in, a jurisdiction associated with higher ML/TF risk. The EMA is aware of product offerings that allow the receipt of funds from and transmission of funds to higher risk jurisdictions – which may present a higher inherent risk. However, firms in the EMA membership will have a risk assessment process in place that will identify and score country risk and where higher risk customer activity is identified, product restrictions will be put in place to further mitigate the risk, and enhanced due diligence (EDD) conducted to understand the rationale including source of funds for the transaction.
2. Which categories of jurisdiction, person, business relationship or product do you consider pose the greatest level of ML or TF risk?	<u>Jurisdiction:</u> E-Money products may be offered to customers from higher risk jurisdictions or be used to make payments to recipients in higher risk jurisdictions. In these circumstances there will be real time monitoring of such activity and where this is effectively performed it may serve to mitigate these risks. However, in circumstances where ongoing monitoring controls are not effective the risks of E-Money being used for ML or TF purposes can be more significant. The EMA has some evidence of potential money-laundering

	scenarios where multiple individuals may be using a single account to transfer funds overseas to higher risk jurisdictions. Where this activity has occurred the customer account itself is suspended and a Suspicious Activity Report (SAR) is submitted to the National Crime Agency. Also once identified the scenario can be added to the transaction monitoring engine to improve the efficiency should it reoccur in the future. <u>Person (Customer):</u> Customer account where significant sums of cash are loaded and/or withdrawn pose a higher risk ML and TF risk. However, customer activity is monitored closely through the use of transaction monitoring either by a rules-based alerts or the use of artificial intelligence driven systems in EMA member firms. Also, customers who change their ID information frequently may pose a higher ML and TF risk but where this occurs, screening is conducted and corroborative evidence from trusted sources where available is sought to mitigate impersonation fraud risk. Customers who do not pass verification screening will be asked for further documentary evidence to support and verify their account application – in the absence of further information the account will not be opened by the EMI. <u>Products:</u> As previously stated, products with greater functionality in terms of offering cross border and P2P payments pose may pose a greater risk. The risk is however only significantly higher where account limits are elevated. This is because most e-money related payments are low in value averaging in the region of EUR 40. However, in the product design phase where these higher risk products are being developed firms will build into the product limits on the functionality to mitigate the opportunities for abuse – ATM functionality may for example be removed or greatly restricted. There are some products that offer the ability to fund the product in cryptocurrency, and these will be expected to trigger additional CDD and EDD obligations as a matter of course. <u>Business relationship:</u> Consumer business relationships are managed on the whole based on the limited values transacted; where these are elevated, then greater scrutiny and individual review would be undertaken. Business relationships with business customers on the other hand, and subject to the full scrutiny and onboarding processes that reflect the degree of risk different customers pose. Due diligence will be conducted on the beneficial owners and directors of such companies as a matter of course. Initial baseline expectations will be set by the type of business, and growth expectations; this will then be monitored individually, and against

	comparators for evidence of departure, when investigation will then be required. If the customer due diligence and subsequent ongoing account monitoring are conducted effectively then this will lower the residual risk associated with this type of account. Companies that may also pose higher risk for member firms are those involved in higher risk business activities such as online gambling, adult entertainment and sale of pharmaceuticals. EMIs may act as merchant acquirers for such business types and where they hold high risk accounts the level of due diligence will need to be commensurate with the risk posed. Normally, higher risk business customers will be subject to enhanced due diligence and ongoing monitoring where source of funds and transactions will be routinely monitored to ensure they are in line with expected turnover values and volumes. Also, information such as charge backs will be monitored as higher levels may be indicative of a merchant that is acting in bad faith or at worst fraudulently. Fraud is a key financial crime risk within the sector and is therefore monitored closely particularly in online merchant payment product offerings. The residual risk lies where such customer types are being offered E-Money services but are not being effectively managed in compliance terms and therefore in these circumstances money-laundering through such accounts could occur. Although the EMA has limited evidence to support this typology within its experience.
3. On what scale have you seen ML or TF activity through the products or services you offer?	As stated for the reasons above, we have limited evidence within our member firms that E-Money products are being widely used for ML and TF purposes. Where suspicious activity has been noted, it has often been related to Fraud as the predicate offence with the proceeds being laundered. The predicate frauds observed where identified have been Impersonation Frauds, Investment Frauds, Social Engineering Frauds and Authorised Push Payment (APP) to be the most common typologies. The common theme in these frauds is the use of social engineering by criminals to dupe customers into either providing their own secure details to allow them to be used to steal funds fraudulently or apply for further credit accounts using stolen customer details. In some cases, the victim will authorise a payment themselves to the fraudsters account believing they are purchasing legitimate goods or services, having been convinced to do so by the fraudster. The difficulty for EMIs with these victim types is that they are not their customers. EMIs rely in this respect on the fraud prevention and education being provided in other parts of the financial services sector.

	The EMA has also noted to a limited extent the use of 'fake' merchant accounts to launder the proceeds crime, where initially the account looked reasonable, offering legitimate services and passing due-diligence procedures. However, monitoring then revealed that the account was in fact selling high-risk or illegal products badged as a different commodity. To identify such cases, EMIs conduct regular account reviews. As far as TF is concerned, the industry has a limited ability to detect this without intelligence information from law enforcement. Common scenarios being used relate to spending in high-risk jurisdictions associated with TF risk in combination with spend types that may be indicative of TF risk. In these scenarios this activity will be investigated by the firm and where necessary a SAR made to the NCA. A case where an e-money instrument was used in the preparation of a terrorist attack involved a fully-verified prepaid card that was used for legitimate purposes such as purchases of food and accommodation.
4. Please tell us about trends in the ML or TF activity you have seen.	Where money-laundering activity has been identified, the prevalent predicate offence is often Fraud. E-Money products can be used to launder relatively low sums before such accounts are identified and blocked by individual firms. The EMA has seen some instances of customers using mail redirection services to mask their location and circumvent the geographic restrictions firms put in place in terms of card/account issuance. The greater use of digital monitoring in addition to established address verification requirements will serve to mitigate these emerging risks. On one occasion, a link with potential human trafficking has been noted in a client scheme aimed at migrant workers, where multiple individuals had accessed a single account and used it to remit funds to higher-risk jurisdictions. This risk is mitigated by limiting the number of accounts with shared credentials, such as addresses, mobile numbers, and email addresses.
5. In your view, to what extent would it be possible to use products and services other than those you've flagged in questions 1-4 to mask the source or ownership of funds or assets, or mask the destination or purpose of funds or assets?	There is limited evidence beyond that covered in sections 1-4 to indicate that any further risks lie in the E-Money sector and its products.

6. To what extent does your organisation have the resource to ensure compliance with AML/CTF regulations? Does your organisation have confidence in its understanding of the risk?	Our member firms have significant resources deployed in compliance functions to prevent ML and TF. This involves a mixture of human and technological resources to further enhance the systems and controls within firms. Each firm conducts business-wide risk assessment and ML/TF risk assessment and then applies a risk-based approach to mitigate inherent risks identified in the products it offers and the underlying customer base. Staff undergo regular AML and CTF training which serves to enhance their knowledge and understanding of financial crime risk and to identify suspicious activity. However, Brexit has increased potentially the risk of fragmentation within firms who are seeking licences in multiple EEA countries. This may stretch existing resources and knowledge held within firms given the variety within each National Competent Authority in terms of regulatory obligations and regulatory reporting. Another resourcing risk associated with Brexit may be that the uncertainty may lead to compliance staff leaving the industry, diluting the already limited pool of suitably qualified staff potentially reducing effectiveness of compliance teams who may need to rely on less experienced and well qualified staff in the interim. However, those member firms who have responded to us have indicated they have adequate compliance resources at present.
7. How do you think the risks identified in your sector in the 2017 NRA have changed since?	The EMA believes the money-laundering risks within the E-Money Sector have reduced since the publication of the 2017 NRA, as reductions in wallet/card limits for Simplified due diligence (SDD) products in 4MLD and 5MLD make e-money products a poor means of laundering cash anonymously. Given the low value of limits, many firms no longer offer SDD products to the market. In the limited circumstances where E-Money products have been used to launder the proceeds of crime, these have often been related to predicate fraud offences. The industry is aware of TF risks and employs real-time, scenario-based transaction monitoring on funds deposited and spent in order to mitigate this TF risk. The EMA notes that since publication of the NRA in 2017 the Financial Conduct Authority has conducted a Thematic Review of the money laundering and terrorist financing risks (TR18/3[1]) within the E-Money sector. The published report was supportive of the E-money sector and indicated that firms in the review were managing

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

	their risks adequately and had effective AML systems and controls to mitigate money laundering and terrorist financing.
8. Have you recognised any emerging risks, that have not previously been identified? Are there any future risks you may foresee?	A longstanding threat that has recently seen a resurgence is the attempted use of 'mule' accounts to launder the proceeds of crime. In these scenarios Fraudsters will often recruit individuals online, with the offer of making money quickly or purchase accounts from students who may be finishing their studies and no longer need their account. In this type of case, individuals will set up an account to receive a transfer into, then use those funds to make deposits with betting companies or distribute them between the accounts of other recruits. The mules themselves are not aware of the source of the funds, or the purpose of the activity, just that they are being paid to do it. However, this risk is mitigated by the creation of rules within transaction monitoring systems to highlight this type of activity and allow the capture of incoming payments before the funds can be distributed. Relationships with such clients are terminated. Also, a SAR will be made to the NCA to report suspicious activity and where possible allow the proceeds of crime to be seized in such circumstances. It may also be identified and prevented through the proactive use of technology to monitor mobile phones and IP addresses associated with an account and alert where these change without good reason. Greater use of 'social engineering' to facilitate the stealing of customers' secure details and encourage customers to make payments to fraudulent recipients is on the rise within the industry. The firms within our membership have fraud controls in place to mitigate the money-laundering associated with such frauds. But they do not have any control over the victims of such scams, as they are often not their customers; the only way to improve the situation is greater emphasis on education and prevention within vulnerable customer groups who are more likely to be within the traditional banking sector.

9. Please provide your assessment of any further factors contributing to the vulnerability of the sector, the likelihood of threats materialising in the sector or anything mitigating the risk within the sector.	For the reasons already stated, the EMA supports the conclusion that the risk levels within the E-Money Sector in terms of ML and TF are diminishing. This is because of the significant tightening of controls around SDD products and the monitoring of card usage in real time. The targeted use of digital identification and verification processes within firms is a key strength within this sector. These processes are used at onboarding to identify and verify new customers and then throughout the customer journey to complement ongoing monitoring efforts. A broad range of customer data is collected that can then be used for due diligence and ongoing monitoring in real time and may be readily retrievable in the event it is required where suspicious activity is identified and crime is investigated. The growing use of digital verification within the sector where external databases are checked to include the use of Application Processing Interface (API) will allow greater reliability and confidence in the process, particularly in situations where the government has moved to create such reliable database sources which can be accessed by firms at minimal cost through an API.