Subject: EMA input for Department of Justice Terrorist Financing Risk Assessment

Date: 20 June 2023

The EMA are grateful for the opportunity to provide responses to the questions posed of PSCF members for the Terrorist Financing Risk Assessment; Our input is below.

1. **What products and sectors of economic activity do you view as high risk and as low risk in Ireland? Please tell us why.**

Our membership is largely made up of e-money institutions, payment institutions and cryptoasset service providers.

- Where activity in these sectors involves small-value payments to merchants for the purchase of goods and services, we do not think it presents a significant TF risk, even though e-money cards may be used by terrorists as by any other person making purchases online or offline. Without specific intelligence, such activity is, however, difficult to detect, as it is often funded by legitimate sources of funds. These sectors therefore rely on information from law enforcement to inform their control processes. They also rely on their own knowledge of their customers and business model to feed their fraud engine, and therefore detect any suspicious transaction. The usual controls apply around high-risk jurisdictions. For merchant acquiring on a digital platform, for example, disbursements are all made within the EEA and IBANs are mandated for disbursements. Furthermore, the merchant acquisition fees imposed can act as a deterrent to bad actors. As a tool for fundraising, it would also be difficult to raise significant amounts of money by placing a digital product onto a marketplace.
- It should be stressed that despite law enforcement's occasional statements to the contrary, scheme-branded, open-loop prepaid cards do not present a higher TF risk because they can be passed from person to person and are less conspicuous that carrying cash across borders. This rests on a misunderstanding of how e-money works; e-money is stored not on the card or device but in a central account, which is monitored in real-time for suspicious transactions. In this aspect, cards function the same as credit and debit cards, which can also be passed to others and easily carried cross-borders. Use in high-risk jurisdictions

will be flagged and prevented, as will be multiple purchases of cards by the same person.

- Cryptoasset transfers are subject to stricter KYC limits than e-money and payment services (including in relation to occasional transactions, the e-money exemption from CDD and the FTR).
- P2P transactions may carry by their nature a higher risk, although all customers are subject to full KYC requirements if a product is to be used for this purpose. Again, intelligence sharing is key for identifying bad actors. Those who are specifically raising funds, such as charities and non-profit organisations, or who may have access to public funds, such as PEPs, are classified as higher-risk customers for both ML and TF, as they could hide behind a legitimate front for fundraising, are easily established and may operate in areas of conflict. Specific processes are implemented by PSPs to mitigate these risks.

2. **Can you tell us of any preventative measures or outreach efforts that are either already in place or which could be introduced to reduce the threat of and/or vulnerabilities to terrorist financing?**

- "PPP" Public private partnerships with government agencies to align on matters relating to TF. A good example is the Ireland Fintech Intelligence Group, where Fintech firms can share and exchange knowledge experience with the local FIU team. In the UK, there is a NCA CryptoCurrency Working Group that has proved useful in information sharing for cryptoasset service providers.
- The 314b process, which is a good example of information sharing with peers from the USA.
- Participation in industry association groups to share typologies with peers, especially the red flags and mitigating factors of those typologies, on a regular basis, has proven valuable, such as the EMA's Fraud Subcommittee.

3. **Can you tell us of any measures that exist or are being put in place to mitigate the risks associated with terrorist financing?**

- Controls around content for which payment is made: Use of monitoring technology to screen content by running keywords and images through algorithms.

- Controls around payments themselves: Enhanced transaction monitoring; screening and reporting with rules on jurisdictions that may be more exposed to TF; verification controls on bank account ownership to ensure payments go to the intended recipient.
- Controls around customers: Screening for PEP and sanctions; EDD on higher-risk categories of customer.
- Specific controls relating to cryptoasset transfers: Blockchain technology means that, in most circumstances, transfers are permanent, indelible, unalterable and publicly open to audit. This means that once a blockchain address has been associated with a financial crime activity, likely by law enforcement, it is possible for investigators in the private and public sectors to follow all the funds that have gone to and from that address at any point in time. For example, blockchain monitoring vendors maintain and develop proprietary databases of blockchain addresses which they identify and label to aid in identifying and managing risks associated with blockchain transfers, including for TF. Cryptoasset service providers can set their controls so that alerts are generated when a client interacts with such addresses, even if such transactions are not directly touching the firm. Transfers that are direct to or from addresses associated with TF risk can be automatically held and not processed until a review is conducted. Additionally, the inception of leading-edge capabilities such strategic intelligence, proactive investigation and incident response teams, offers further opportunities to identify and mitigate TF risk. Firms' strategic intelligence teams monitor for financial crime threats and typologies extant and emerging in internal casework and across the wider industry. These insights are used as a basis for internal threat assessments, enabling firms to assess the effectiveness of their controls and informing their risk-based approach to control enhancements. These controls and capabilities, along with the opportunities provided by blockchain forensics, are significant advantages when seeking to mitigate TF risk.