16 November, 2023

Tether Operations Limited
c/o SHRM Trustees (BVI) Limited
Trinity Chambers, PO Box 4301
VG1110, Road Town, Tortola
British Virgin Islands

The Honorable Cynthia Lummis
United States Senate
127A Russell Senate Office Building
Washington, DC 20510

The Honorable French Hill
United States House of Representatives
1533 Longworth House Office Building
Washington, DC 20515

Dear Senator Lummis and Representative Hill:

I respectfully write today on behalf of Tether to address the concerns and questions you raised in your letter to Attorney General Merrick Garland dated October 26, 2023. Due to the gravity of such concerns, it is paramount that we provide a detailed and comprehensive response.

Tether is fully committed to the fight against terrorist financing, compliance with the Bank Secrecy Act and U.S. Sanctions Laws, and meeting the highest levels of customer due diligence and rigorous transaction screening. As I explain below, Tether has a robust KYC, BSA compliance, and transaction monitoring program, sophisticated third-party systems for that monitoring, and a proactive approach to identifying suspicious accounts and activity. Equally important, Tether has a long history of cooperating with law enforcement and anti-terrorist financing agencies throughout the world and acts upon requests to freeze addresses based on that cooperation. We have always assisted law enforcement when called upon to act, and we remain fully committed to continuing to work proactively with agencies globally. Tether has and will assist in identifying and freezing addresses subject to sanctions, engaged in illicit activity, or engaged in any form of terrorist financing.

Tether's KYC and Compliance Efforts

There are some facts that we would like to review and clarify in order to address the concerns expressed in your letter. First, it is important to understand the full scope of Tether's Compliance and KYC/AML efforts. Tether has a sophisticated Compliance Department and a strong KYC/AML program staffed by experienced industry professionals from major international financial institutions. Tether is committed to enhancing these efforts with significant investment in world-class third-party technology consultants. As a Money Service Business registered with FinCEN, the KYC/AML compliance team at Tether applies the same KYC/BSA standards for clients that seek to do business with Tether that you would see at sophisticated financial institutions, including a full review and background check of each potential customer, a review of their source of funds, a check against any potential sanctions lists, including both OFAC and EU sanctions, a review of any negative news or other information that would connect a potential customer with illicit activity, like terrorist financing, money laundering or other potentially criminal activity. Consistent with the actions of financial institutions, Tether uses well-known and respected third-party services like WorldCheck and Chainalysis to perform due diligence and background checks. Our team also uses these services to run continuous news and information searches on existing

customers to ensure we have the most up-to-date information on clients and that their profiles have not changed.

Tether's compliance program is also subject to independent review. The IRS has conducted a Title 31 examination of our KYC program on behalf of FinCEN. Tether has also retained a prominent Washington DC law firm to conduct an Independent Review of our KYC/AML, BSA, and On-Boarding program to ensure they are of the highest standards.

Primary Market Activity

I would also like to directly address your concerns about whether Tether has assisted in facilitating any terrorist financing or whether customers were engaged in or facilitated terrorist financing or other illicit activity. As mentioned above, before Tether creates or redeems USDT for any individual or entity (our customers), it conducts a thorough KYC and due diligence review. As a result, Tether can confirm that we are not aware of any evidence that any customers have ever been part of, or have supported any terrorist activity, nor are they subject to sanctions. Tether can also confirm that it has not sold any USDT to any sanctioned addresses or customers, or anyone linked through our diligence to terrorist financing.

Another important clarification is that, differently from the most prominent cryptocurrency exchanges that onboard millions (and sometimes tens of millions) of customers, Tether's primary market customer base is mostly composed of accredited individuals, trading firms, and institutions. Since Tether's customer base can be counted in the thousands, rather than millions as most prominent cryptocurrency exchanges, Tether performs much more thorough due diligence on all its customers.

Tether has also recently opened a discussion with Chainalysis to evaluate a comprehensive independent analysis of the activity of USDT across the major blockchains it has transacted on in order to ensure that USDT has not and is not used for terrorist financing or the facilitation of terrorist financing. Moreover, Tether is reviewing new bespoke tools provided by Chainalysis to further enhance real-time monitoring capabilities.

Surveillance Monitoring Tools

Tether's reviews do not end at the onboarding of clients. Tether utilizes state-of-the-art third-party surveillance monitoring tools to continually monitor clients engaged in the creation and redemption process. In particular, Tether uses the Reactor tool from Chainalysis and receives secondary market risk reports from this Company. These surveillance tools are considered to be the leading options for blockchain surveillance and are used by many U.S. government agencies to surveil activity on the blockchain.

Tether utilizes the tools to monitor and identify the transmissions of USDT across multiple blockchains and identify suspicious or high-risk activity, including mixers, high-risk exchanges, SDNs or other sanctioned wallets, or wallets linked to terrorist financing. The Reactor tool allows Tether to analyze transactions across the blockchain to identify potentially problematic wallets or wallets linked to funding of Hamas, Hezbollah, the Palestinian Islamic Jihad, and other terrorist organizations. The results of this surveillance are actively used by Tether to close accounts, freeze tokens, and report suspicious activity by filing SARs with the appropriate regulatory agency.

In addition, Tether remains fully committed to using these tools to identify potentially suspicious transactions. We proactively reach out to law enforcement and anti-terrorist financing agencies and inform them of suspicious activity or wallets.

As an example, Tether recently worked with the U.S. Secret Service on a large investigation relating to so-called "Pig Butchering," whereby we proactively provided the Secret Service with information that appeared suspicious and potentially linked to fraud. This investigation is not related to Tether customers, but rather we took it upon ourselves to identify various risks and inform the DOJ and U.S. Secret Service about secondary market risks. Collaboration on this investigation is ongoing.

These tools and strategies are not just preventative, but also investigative, aiding law enforcement by providing critical data and analysis when suspicions arise. Our efforts help trace the path of Tether tokens as they change hands, offering an extra layer of security that complements the checks implemented by secondary market operators. Through this collaboration, we aim to set a standard that not only meets the requirements set forth by regulatory bodies but also establishes the right benchmarks for security and vigilance in the digital currency market.

Law Enforcement and Anti-Terrorist Financing Cooperation

Tether has a long history of cooperation with various law enforcement agencies – as we provide information, and freeze assets in requested wallets. Tether has collaborated/worked with law enforcement agencies in 19 jurisdictions globally to assist in investigations of illicit activity, including terrorist financing. In particular, Tether has regularly cooperated with the Department of Justice in a number of investigations and has frozen USDT addresses at their request.

As a result, Tether has frozen over 800 million USDT in secondary market addresses, the majority of which was connected to thefts, particularly blockchain and exchange hacks. Specifically, Tether has helped the DOJ with 68 separate requests, resulting in the freezing of 188 addresses, holding ~70,000,000 USDT at the time of freezing. Tether has also worked with law enforcement agencies, including Israel's anti-terrorist financing agency, the NBCTF, to identify and freeze addresses linked to Hamas and other terrorist financing. Tether has worked with authorities in Israel and Ukraine, to identify and freeze 32 addresses, halting 873,118.34 USDT. Tether's collaboration with the NBCTF predates the heinous attacks of Oct 7, 2023. We have worked with the NBCTF to freeze terrorist-affiliated addresses before the attacks and have and will continue to work closely with them in the future. Our work with the NBCTF and other agencies globally is evidenced in the Telegram group for the prominent public crypto fundraising campaign operated by Gaza Now, which has explicitly asked its donors to stop sending USDT as these tokens are prone to being frozen.

Tether remains fully committed to continued cooperation with all enforcement and anti-terrorist financing agencies to ensure USDT is not used to support terrorist activities, terrorist financing, or any criminal activity.

We would also respectfully like to bring to your attention two independent analyses of some of the questions raised in your report. Both Chainalysis and Elliptic, two leading investigative firms that analyze blockchain activity, have reviewed the role of cryptocurrencies like Tether in terrorist financing. In the report titled *Correcting the Record: Inaccurate Methodologies for Estimating Cryptocurrency's Role in Terrorism Financing*, dated October 18, 2023, Chainalysis commented that not only was the role of cryptocurrency overstated in terrorist financing, but that cryptocurrency's transparency and traceability could directly aid in the fight against terrorist financing:

> Given blockchain technology's inherent transparency and the often public nature of terrorism financing campaigns, cryptocurrency is not an effective solution to finance terrorism at scale. However, even small amounts of funds sent to terrorists can do tremendous damage. When investigating small inflows of funds to terrorism campaigns, law enforcement and intelligence agencies can leverage blockchain analysis to investigate donors, facilitators, and cash-out points

and partner with private sector organizations to shut down activity. This kind of work has led to seizures of funds related to Hamas, Hezbollah, and other terrorist groups. These successes demonstrate that it is possible to understand and disrupt the financial networks that support terrorism.

As noted above, Tether remains fully committed to working proactively with law enforcement and other anti-terrorist financing agencies across the world to stop the use of USDT in any illicit activities. Our commitment includes working with those agencies to freeze USDT, just as we have done in the past. Tether also remains fully committed to maintaining the highest standards of compliance with applicable BSA and KYC standards, ensuring compliance with all applicable AML and anti-terrorist financing laws and directives, and providing the public, as well as your offices, transparency around these efforts.

Conclusion

Our proactive measures and collaborations reflect Tether's unwavering commitment to not only comply with but also to actively support the enforcement of laws and regulations. In our collaborative endeavors, working alongside law enforcement agencies aligns with our core values of trust, transparency, and responsibility.

In summary, Tether remains fully committed to meeting and exceeding its legal and ethical standards and obligations. By initiating and maintaining a proactive approach, we aim to assist law enforcement in preventing financial crime and deterring terrorist financing. It is through these efforts that Tether reinforces its commitment to maintaining the integrity, transparency, and trustworthiness of the Tether ecosystem, a sentiment echoed in every action we take to detect, deter, and disrupt illegal activities within the cryptocurrency space.

We remain committed to financial integrity, transparency, and probity. We value our collaborative relationship with regulatory authorities and remain committed to working with them to foster a continued environment of trust and understanding.

Sincerely,

Paolo Ardoino
CEO
Tether

cc: Chairman Sherrod Brown, U.S. Senate Committee on Banking, Housing, and Urban Affairs
Ranking Member Scott, U.S. Senate Committee on Banking, Housing, and Urban Affairs
Chairman McHenry, U.S. House Financial Services Committee
Ranking Member Waters, U.S. House Financial Services Committee