October 25th, 2023

**Written testimony on "Combating the Networks of Illicit Finance and Terrorism"**

**Before the Senate Committee on Banking, Housing, and Urban Affairs**

**By: Dr. Shlomit Wagman**

I am honored to present my expert opinion before the distinguished Committee regarding the combat against networks of illicit finance and terrorism.

As one of the experts who participated in the design of the international regulatory approach to virtual assets, as well as gained practical experience while leading numerous financial investigations of money laundering and terrorism financing, I am honored to share with you several insights and offer actionable proposals both domestically (in the US and elsewhere) and globally (through multilateral efforts, such as within the framework of the FATF).

I've served as the Chair of the Israeli Money Laundering and Terrorism Financing Prohibition Authority and was also the Co-Chair of the *Financial Action Task Force*'s (FATF) Risk, Typologies and Methods Working Group. While serving in these capacities, I managed dozens of terrorism financing investigations and shaped global and national policy in the field. In addition, I led the Israeli accession to the FATF following a thorough evaluation process in which Israel achieved a (rare) High Effectiveness rating regarding the use of financial intelligence, terrorism financing investigations and confiscation. Currently, I am an affiliated scholar with the Mossavar-Rahmani Center for Business and Government and the GETTING-Plurality Network at the Harvard Kennedy School and the Berkman-Klein Center at the Harvard Law School. I am also a senior executive at Rapyd, a global payment company.

The opinions presented in this testimony are my own and should not be attributed to any of the institutions with which I am affiliated with.

## A. Background

Quite simply, funding is essential for the operations of terrorist organizations. Conversely, the disruption of funding channels used by terror organizations plays a pivotal role in countering (and even abolishing) their activity.

Looking specifically at Hamas and Hezbollah - both function like any other terror organizations. For example, the horrifying terror attacks of October 7th demonstrated the extent to which Hamas adopted the ISIS playbook: Hamas slaughtered innocent civilians in a brutal and well-organized attack.

This extensive operation, in which thousands of terror activists took part, required substantial funding for vehicles, weapons, drones, tracks, explosives, tunnels, logistic support, and more. In addition, substantial funding is likely required by Hamas to finance its continued holding of the 200+ hostages (from 33 countries) kidnapped from their homes and taken to Gaza.

My goal in today's testimony is to review the funding channels used by illicit and terror organizations and – as per your request – focus specifically on the use of cryptocurrencies, which most likely funded (both directly and indirectly) Hamas's activities.

This testimony document outlines the following:

- Surveys the main legal framework and regulatory requirements found in the domain of anti-money laundering and counter-terror financing (AML/CFT) with respect to terrorism financing.
- Discusses current terror financing trends. In light of the October 7th attacks, and at the request of the Honorable Committee, this discussion focuses on Hamas current terrorism financing trends, existing legal frameworks, and gaps and challenges in the specific context of virtual assets.
- Proposed actions that can be taken in the domestic sphere (such as by the US and other countries) and in the international sphere to strengthen the existing legal framework and target the very gaps in this framework that are exploited by terror organizations like Hamas and Hezbollah.

## B. Legal Framework Background - The Global Combat Against Terrorism Financing

After the 9/11 attacks, a global unified framework was designed to combat terror financing using the same toolbox previously developed to combat money laundering. This toolbox included the imposition of administrative obligations on the private sector (such as monitoring customer activity and reporting suspicious transactions to designated intelligence and law enforcement authorities) and requiring sovereign countries to establish financial investigation, enforcement and punitive capabilities, including confiscation of funds.

This global response was designed by the Financial Action Task Force (FATF), the international watchdog in the field. Today, the FATF is composed of thirty-nine member countries (including most of the G20 countries) and regional organizations, and together with its nine associated FATF-Style Regional Bodies (FSRBs), it encompasses over 200 jurisdictions.

The FATF has defined global mandatory standards in the domain of Anti-Money Laundering and Counter Financing of Terrorism (AML/CTF) that all jurisdictions must implement into their national legal systems and ensure their effective enforcement. The FATF and FSRBs conduct ongoing monitoring to review and evaluate the level of compliance of countries with these standards, when non-compliant jurisdictions may be listed on the infamous gray or blacklist. These lists are powerful signaling tools that put severe pressure on the listed jurisdictions to quickly meet FATF standards, as the listed jurisdictions are marked as high-risk territories for AML/CFT purposes, limiting their respective financial sectors' ability to participate in the global market. A place on the blacklist practically limits financial activities dramatically between the financial institutions in the blacklisted country and other jurisdictions.

The Global AM/CFT Approach to Virtual Assets

Cryptocurrencies pose substantial challenges to national security and the integrity of financial systems. Certain unique characteristics make them appealing for conducting illegal activities: (1) they are decentralized, unsupervised by any government or central bank, and therefore, like cash, preserve a high degree of anonymity; (2) they are virtual and therefore generally unbounded by geographical borders; and (3) they do not require transactions be conducted in-person. At the same time, they are also reflecting financial innovation, with the potential to initiate a revolution in the way society transfers value, facilitate international commerce and cross-border financial activities, decrease transaction costs and barriers, and enhance financial inclusion.

The FATF was the first international organization to develop a holistic strategic response to cryptocurrency risks. In 2018, the FATF amended its mandatory standards to explicitly apply cryptocurrency to its rules, and subsequent updates and clarifications. The FATF's regulatory approach to cryptocurrency is similar to the approach it has taken to regulating traditional financial activities. The FATF requires countries to impose the full AML/CFT framework, albeit with relevant modifications pertinent to cryptocurrencies' unique technological characteristics.[1]

As it has done when regulating other financial activities, the FATF identified virtual asset platforms capable of monitoring the financial activities conducted through their systems, termed "**Virtual Assets Service Providers**" (VASPs). This term was defined

[1] To ensure that the regulations are as effective as possible, and to avoid circumvention of its global Recommendations, the FATF defined cryptocurrency assets broadly. FATF chose the term "Virtual Assets" (VA) rather than "cryptocurrency" or "digital asset" to refer broadly to any "digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes." The definition does not include the digital representation of fiat currencies.

broadly to capture all relevant services, including virtual currency exchanges and certain types of wallet providers.

All jurisdictions must establish licensing or registration requirements for VASPs. At a minimum, VASPS must be licensed where they were legally created. Some jurisdictions may also require licensing or registration as a condition for conducting business. VASPs should be subject to the full range of preventative measures and AML/CFT obligations, similar to other financial intermediaries. These obligations include, among others, the requirements of conducting customer due diligence and ongoing monitoring, recordkeeping, submitting of suspicious transaction reports (STR) to the designated Financial Intelligence Unit (FIU), and screening customers and transactions against designation lists. In order to conduct the needed examinations as part of the consumer due diligence and licensing process, the FATF recommends using relevant tools and resources, such as **blockchain analytic tools**. Given the cross-border nature of VASPs' activities, the FATF is required to impose additional preventive measures, for example conduct Customer Due Diligence for every transaction above $/€1,000.

In addition, the FATF adopted a "Travel Rule" requirement for VASPs. The Travel Rule, a modification to its approach regarding wire transfers, requires VASPs to obtain, hold, and transmit required originator and beneficiary information, immediately and securely, when conducting VA transfers. These are the same obligations traditional financial intermediaries are required to undertake when they transmit transaction information via SWIFT (in a way which is compatible with data protection and privacy laws).

Investigative Aspects of Virtual Assets

Aside from the risks associated with virtual assets, their digital environment actually provides unique opportunities for law enforcement agencies (LEAs) to conduct financial investigations. Analysis of public blockchain ledgers allows both the private sector (VASPs and other financial institutions) and LEAs to trace financial activities over the public blockchain and identify connections to suspicious transactions and illegal activities even if the cryptocurrency holder is represented only by a wallet number. The public ledgers allow analyzing and tracing a long history of transactions, thereby identifying whether the funds were involved in a known illicit activity, co-mingled with illegal funds, processed by an unregulated VASP, or were suspiciously treated (e.g., they were treated with an anonymity-enhancing mixer). In addition, because the data is available in digital format, analysts can apply sophisticated techniques to process and analyze it. At the same time, it is important to note that blockchain analytics is not a silver bullet. Private ledger cryptocurrencies, such as Monero, provide very limited public information.

When VASPs collect data pursuant to their AML/CFT obligations, the data can provide the linkage between pseudonymous wallets and identifiable entities, especially when virtual asset holders cash in/out from/to fiat currency. The information collected by VASPs as part of their customer due diligence obligations includes a vast

repository of revealing data, including government- issued identification (which is often crossed with biometric data), geographical location, IP addresses, statements regarding the source of funds, beneficial owners, and VASP-identified concerns based on the consumer or transaction's nature. This information can be obtained by LEAs as a result of spontaneous reporting by VASPs to the relevant FIU, or following a request by an LEA (either a request for additional information by the FIU or a court-issued warrant). When the financial intelligence held by LEAs is combined with other relevant intelligence (such as open-source intelligence (OSINT)), signals intelligence (SIGINT), and human intelligence (HUMINT), it empowers LEAs to trace suspicious financial activities and unmask the lawbreakers.

Implementation of the FATF Standards by Countries - Statues and Gaps

So far, only a limited number of countries have implemented this framework.

As of June 2023,[2] four years after the FATF's adoption of standards on VAs and VASPs, **75% of the countries that went through their routine reviewing process have not implemented the framework in full**. In addition, one-third of the countries have not conducted a risk assessment, and a similar number have not yet decided if and how to regulate the VASP sector.

Moreover, more than half of the countries **have not taken any steps towards Travel Rule implementation**.

It should be highlighted that this situation has a major cost. Platforms that are not subject to the full extent of FATF standards are becoming crypto mixers, as it is almost impossible to track the illicit assets inserted or transferred via the platform. This continues to make the use of VASPs attractive to terrorist organizations.

## C. Current Trends in Hamas Terror Financing

*Hamas – General Sources of Funding*

Hamas is designated as a terror organization by the US, EU, UK, Australia, Canada, Israel and other countries. Unlike ISIS, it has not yet been designated by the UN as a global terror organization, hence the financial sanctions toolbox is somewhat limited, as described below.

Hamas's funding resources include the following main channels:

- **State funding**, which is transmitted mainly by cash, cross-border payments, Hawala, trade-based terrorism financing, money exchanges and banks.
- **Business portfolios**, including real estate and investments.

[2] https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/June2023-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf

- **Fundraising**, including through social media platforms and crowdfunding campaigns in which money is transmitted via bank accounts, payment services and crypto exchanges.
- **Humanitarian aid**, which is misappropriated to and stolen for its own activity.

*Hamas's Use of Virtual Assets*

Hamas was an early adopter of virtual assets, using them to circumvent global supervision on money transfers and to raise funds. In recent years, tens of millions of dollars in virtual assets were identified as being linked to Hamas, however, only a small portion of these funds were successfully confiscated, as detailed below.

Starting in 2019, Hamas has been fundraising in cryptocurrency. Initially, , Hamas received a relatively small donation of several thousands of dollars in Bitcoin. It used regular cryptocurrency wallets, later moving to non-custodial wallets, and then in 2021 adopted more advanced techniques, generating a unique address for each new donation.

In the summer of 2021, after a conflict with Israel, Hamas solicited increasing sums in Bitcoin. By July 2021, following Israel's designation of Hamas crypto wallets, more than **$7.3 million worth** of virtual assets were seized. The designation included over **20 different types of virtual assets**, including Bitcoin, Ether, Tether, TRON, Cardano, XPR, Dogecoin, and more.

In April 2023, following a further series of Israeli asset freezing orders and seizure of many accounts, Hamas announced to its supporters that it would stop receiving fundraising via the crypto currency Bitcoin, citing an increase in "hostile" activity against donors and that "this comes out of concern about the safety of donors and to spare them any harm".[3] **Such a statement demonstrates that the FATF approach of signaling to the market of "blacklisted" crypto, was proven to be efficient**.

On October 10th, 2023, after the recent terror attacks, Israel police froze the cryptocurrency accounts that Hamas was using to solicit donations on social media to support it during the war.[4]

It is important to note that after each designation of a Hamas wallet became public, many VASPs, regulated and non-regulated, identified connections to the designated wallets and shared additional information with the Israeli authorities. Some sources communicated the information directly to Israel, to the National Bureau for Counter Terror Financing (NBCTF), while others informed the relevant LEAs in their respective jurisdictions or disseminated suspicious transaction reports to their own FIU, which in turn cooperated with the Israeli FIU and other relevant LEAs. The valuable information provided by VASPs around the globe included significant data they gathered by following their AML/CFT obligations, as well as through open-source

[3] www.reuters.com/world/middle-east/hamas-armed-wing-announces-suspension-bitcoin-fundraising-2023-04-28/
[4] www.reuters.com/technology/israel-freezes-crypto-accounts-seeking-hamas-donations-police-say-2023-10-10/

information and blockchain analytics, and greatly assisted in tracing relevant wallets and seizing related funds.

Additionally, blockchain analytics companies conducted independent research regarding the designated wallets, revealing connections to additional wallets associated with the designation and with previous terror financing investigations. Most findings became public when the companies published their investigations, which assisted in revealing new links to relevant suspected terrorism financing activities.

*Hamas Fundraising Via e-Commerce and Technology Platforms*

According to open-source intelligence, Hamas collects funds using social media and commercial platforms. They direct supporters to purchase certain goods and services via e-commerce platforms, centralized and others that connect buyers and sellers. No real goods change hands and the money is funneled to Hamas.They are relying on the relatively low onboarding KYC examination performed by those platforms, which are mainly lacking the context of the overall transaction.

*Humanitarian Fundraising Campings*

Hamas is known to lead a variety of fundraising campaigns on social media that seem to be legitimate humanitarian campaigns, and linked to charity organizations, making it difficult to trace by the intelligence community, the private sector and donors.

After being published on social media, mainly via Telegram, the donations are being collected in bank transfers, payment transactions, and crypto.

*Hamas Use of Trade-Based Terrorism Financing*

Another typology which is constantly identified as being used by Hamas is “trade-based” financing, which is very similar to the “trade-based” money laundering” typologies.[5]

The typical use case would be state-sponsored funding which is sent, either in cash or Hawalla, to another country. Hamas is purchasing goods, and shipping them to Gaza. The products imported to Gaza are being sold and the cash proceeds are being collected by Hamas in Gaza. Many cases were inspected in which Hamas was using trade and commerce of physical goods to transfer value to Gaze, including toys and chocolate.[6]

[5] FATF report: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Trade-Based-Money-Laundering-Trends-and-Developments.pdf.coredownload.inline.pdf

[6] IMPA report (in Hebrew): https://www.gov.il/BlobFolder/dynamiccollectorresultitem/red-flags-typology-terror-financing-impa-080822/he/professional-docs_red_flags_typology_terror_financing_impa_080822.pdf at p.9.

## D. Proposed Action Items Going Forward:

My testimony above surveyed the global AML/CTF legal framework and the current trends in terror financing by Hamas (including the methods in which Hamas funds its own activities and, likely, the October 7 attacks). In this chapter, I propose several practical operative actions that can be taken, both by the international legal community and the US, to further strengthen the international community's ability to disrupt terror financing channels and – ultimately – the financial ability for terror organizations to carry out their activities.

### *A. Strengthening the Global AML/CTF Regime for Virtual Assets*

- The issue. Many countries have yet to implement the FATF's regulatory framework regarding virtual assets and, particularly, the Travel Rule and inspections on licensed exchanges. This regulatory arbitrage creates a major loophole in the global regulatory regime by allowing for "weakest link" jurisdictions. The result is that illicit and terror organizations "forum shop" and exploit exchanges based in jurisdictions with weak oversight. In addition, no global response is available in real time to such illicit activity and there is no united coalition to promote a response.

- Proposed measures – global level. The following measures are proposed to help strengthen the existing regime and support better implementation and enforcement in jurisdictions with weak oversight:
    - The FATF must take an aggressive approach to enforcing its global AML/CTF framework and work towards closing the global regulatory arbitrages which create the "weakest links." This includes:
        - (i) creating a public "gray list" of countries that have not yet adopted and implemented virtual asset-related controls, such as the "Travel Rule,"
        - (ii) ensure that countries are effectively supervising their licensed VASPs and imposing dissuasive sanctions for non-compliance, and
        - (ii) imposing its customary sanctions regarding non-compliance on such countries (for example, recommending that member states impose advanced due diligence standards and suspicious activity reporting requirements on financial institutions engaged in virtual asset transactions with gray-listed countries).
    - The FATF should further recommend additional measures to regulate Peer-to-Peer, De-Fi and smart contracts.

- Proposed measures – domestic level. In the absence of appropriate response by the regulating county in which an exchange is licensed, or in case of a non-regulated exchange, it is proposed that countries will consider designating the exchange itself, to avoid its use as a "mixer" to launder the funds.

*B. Real-Time Collaboration and Information Sharing re Virtual Assets*

- Issue #1: Due to the rapid and cross-border nature of payment services and virtual asset transactions, there is a need for 24/7 international collaboration between intelligence and law enforcement authorities to identify, freeze and disrupt the flow of funds.

- Proposed measure: Establish mechanisms for collaboration between intelligence and law enforcement authorities, similar to the case of ransomware and other social engineering fraud.

- Issue #2: Public authorities require a more effective channel with the private sector, as most of the data relevant to crypto-related investigations is publicly available (over blockchain) and can be analyzed by the community.

- Proposed measures: Law enforcement agencies (LEAs) should establish channels for rapid information sharing with the private sector and, in particular, with financial institutions, "RegTech" companies, and blockchain analytics experts, about the up-to-date trends used by designated terror organizations. In this regard, Financial Intelligence Units (FIUs), who receive financial intelligence from the private sector, should actively share with the private sector the red flags, typologies, relevant keywords and even "name codes" which are indicative of illegal donations that are channeled to terror activity. The information sharing does not have to be public, but can be done with entrusted RegTech companies.

- FIUs should also publish lists of bank accounts, payment accounts and crypto wallet details which they have identified on social media or otherwise, block them and alert the entire financial system, on an ongoing and consistent basis.

- To make screening more effective for financial institutions, FIUs should make lists accessible in different formats and languages, with as many identifying data points as possible so that private sector organizations can effectively screen, regardless of their size or ability to dedicate resources to compliance.

*C. "Sanctions" Designations*

- Issue: Hamas is currently designated by the US, EU and other countries, but not by the UN. Therefore, it is not necessarily screened in all countries and in relation to different currencies.

- Proposed measures:
    - A proposal for the UN Security Council should be submitted to designate Hamas as a terror organization, as was the case with ISIS. Such action will ensure that Hamas's financial activities will be screened and frozen by all financial systems, in a unified and automatic manner, across all countries, even in those institutions that are physically removed from the conflict zone or may have limited awareness of the nature and type of the terror

financing typologies (as is common), or may be operating with different currencies.
    - Countries that have already domestically designated Hamas, such as the US, EU, and others, should instruct their enforcement agencies to focus on enforcement relating to this specific designation and consider adding additional measures as a policy matter. The US designation of a group of Hamas leaders made on October 18th is a positive, if belated, step. More actions of a similar nature are required.
    - Additional designations should be considered as well, for example, charity organizations that were designated by Israel based on relevant intelligence that connect them to the terror activities.

*D. Improving Financial Investigations Capabilities – Domestically*

- Issue: FinCEN currently does not have authority to ask for additional complementary information from financial institutions or to freeze funds related to terrorism financing, which are crucial operative capabilities needed to disrupt terrorism.

- Proposed measures: The following measures are proposed to help strengthen FinCEN's ability to effectively collect financial intelligence information from financial institutions and to take swift (if temporary) action to disrupt terror financing:

    - FinCEN should be granted with the legal authority to compel all financial institutions to provide additional supplementary information (as opposed to requesting such institutions to do so voluntarily, which is the current situation). This is especially important in the domain of virtual assets, where many different VASPs and other financial institutions are involved.
    - In addition, FinCEN should be granted the legal authority to order an administrative freeze on terror-financing related funds for specified limited periods of time (e.g. 24-72 hours). Similar mechanisms exist throughout EU member states, which enable local authorities to respond swiftly to fast-moving funds, which is normal in today's markets, and to disrupt terrorism financing efficiently.

*E. Risk Assessments of High-Risk Jurisdictions*

- Issue: Key stakeholders in the public and private sectors can serve as gatekeepers or a "first line of defense" against the exploitation of financial and monetary markets by terror organizations. To do this effectively, they need to understand the risks emanating from high-risk jurisdiction, identify their organizational appetite for risk; review their operations to identify exposure to terror financing risk; and adopt risk-management controlling measures.

- Proposed measures:
    - A clear, professional analysis of the risks emerging from high-risk countries (from the perspective of terror financing) should be made available to stakeholders in both the public and private sectors. This will help facilitate

the “risk management” process described above, including establishing effective management of risk appetite, risk exposure and risk-management controlling measures by these stakeholders.

- Ensuring that the FATF (and other parallel institutions) are working in a transparent and credible manner to undergo and swiftly publish their evaluations of countries that are at high-risk for terror financing.
- In this regard, there is a need to mention the concerns that were raised over the past few years regarding the professional capability of the MENAFATF, which is the FSRB mostly relevant to jurisdictions exposed to high risks of terror-financing (such as Lebanon, the Palestinian Authority, and Syria). It is critical that evaluations of these countries are supported by appropriate and professional experts.
- For example, Hezbollah is a major stakeholder in the Lebanese economy. Thus, it is critical that the ongoing MENAFATF review of Lebanon will include a clear and reliable review of its implication on Lebanon economy and its potential exploitation to TF risks and funnel economic resources to Hezbollah.
- In addition, the global financial community requires more clarity regarding the financial ecosystem of the Palestinian Authority and Gaze to allow it better manage TF risk. For a variety of reasons, the PA has not gone through an objective international assessment regarding their compliance with global AML/CTF standards as set by the FATF. Based on publicly available information, I estimate that the outcome of such an evaluation would have likely been unsatisfactory and would have led to the PA being placed on the FATF’s “gray list.” The result of such a listing is that countries which implement FATF-recommended controls would require their domestic financial institutions to impose enhanced measures in relation to transactions with the Palestinian Authority (for example, reporting transactions exceeding certain monetary thresholds). Moreover, a reliable evaluation could have assisted in mapping the compliance gaps in the Palestinian Authority’s financial system and clarifying how sources of funds enter Gaza without supervision and get distributed through illicit channels to Hamas (a situation that is common to the provision of humanitarian aid to Gaza). Such an evaluation, if conducted by a credible and professional team, needs to be conducted without undue delay.

*F. Following additional funding channels and social media platforms*

- Issue #1. Hamas was recently inspected to expand its activities to commerce and technology platforms. This typology can be seen, for example, in temporary housing websites etc. Those platforms have limited ability to identify and monitor risks, and additional discussion on this is required.
- Proposed measures.It is suggested to consider

- Issue #2. Certain social media platforms, such as Telegram, are hosting a substantially large volume of terrorism financing solicitation.
- Proposed measures.

- The EU's Digital Service Act enforces on large social media platforms certain liabilities, including to ensure the content is not infringing the safety of the public and does not call to illegal activities etc. This applies, among others, to Meta, TikTok and such. A reduced level of responsibilities and liabilites is imposed on "host" platforms, such as Telegram, to the content included there. A further discussion is needed on this topic, including references to explicit solicitation for terrorism financing.

Dr. Shlomit Wagman, October 25th, 2023
www.linkedin.com/in/wagman