

TERRORIST USE OF CROWDFUNDING: TERROR FINANCE WATCHDOG ISSUES REPORT ABOUT POPULAR FUNDRAISING VEHICLE

BY NICKI KENYON AND JOSH BIRENBAUM

NOVEMBER 29, 2023

The Financial Action Task Force (FATF) is the global money laundering and terrorist finance watchdog. It consists of representatives from 39 national governments and regional organizations and sets international standards for financial integrity.¹ In October, FATF released its report on the use of crowdfunding platforms by terrorist and extremist organizations.² This memo summarizes the report’s key findings and provides recommendations to make them accessible to a wider audience.

Crowdfunding involves raising money for a project or venture, often via small amounts from large numbers of contributors and through dedicated platforms on the internet. This activity is legal, and numerous worthy causes, startups, small businesses, and nonprofit organizations have used crowdfunding to obtain critical resources. However, the lack of transparency on certain platforms and fragmented data about who is sending and receiving money make these platforms attractive to terrorist organizations and other illicit actors.

As the landscape of global payment and financial technologies continues to evolve, so do the mechanisms through which crowdfunding is possible. This presents new challenges for oversight and requires firms, financial institutions, and law enforcement agencies to keep abreast of rapid changes that will facilitate the use of crowdfunding platforms by both legal and illicit actors.

CHARITIES AND NONPROFITS

Terrorists and violent extremists often raise funds via charities and nonprofits that use crowdfunding platforms to exploit humanitarian causes, taking advantage of donors’ compassion while using their contributions to fund illicit operations. The nominal goals of such deceptive crowdfunding may be to support sporting events, social or medical support, humanitarian aid, or building infrastructure.

Charities that serve as fronts for terrorist organizations may undertake humanitarian relief while diverting a portion of the funds for terrorist activities. For example, the Bush administration in 2001 designated the Holy

.....
1. “FATF Members,” *The Financial Action Task Force*, accessed November 16, 2023 (<https://www.fatf-gafi.org/en/the-fatf/who-we-are.html>)
2. “Crowdfunding for Terrorism Financing,” *The Financial Action Task Force*, October 2023. (<https://www.fatf-gafi.org/en/publications/Methodsandtrends/crowdfunding-for-terrorism-financing.html>)

Land Foundation — the largest Islamic charity in the United States — a terrorist organization and seized its assets.³ A federal grand jury in 2004 charged the organization and five former officers and employees with providing material support to Hamas by distributing funds through charity committees in the West Bank that paid stipends to the families of suicide bombers and Hamas prisoners. The defendants were convicted in 2008.⁴

Nonprofit organizations may also unwittingly be exploited by terrorist organizations, especially if they operate in high-risk locations, by becoming victims of extortion or skimming.

THE CROWDFUNDING-SOCIAL MEDIA NEXUS

More than 1,400 crowdfunding platforms operate globally, and many of them provide donors with the option of giving on a subscription basis in addition to one-time donations. Users can also custom-build their own crowdfunding platforms or websites by using online applications or open-source code. Social media sites and messaging apps enable users to connect with local or global communities, amplify their message, and generate momentum for their causes, reaching a far greater number of potential donors.

Some social media sites and messaging apps offer encrypted messaging services to secure conversations and documents, which terrorists may employ to share financial data, campaign information, and donation instructions. Social media sites may also allow donors to contribute directly through their platforms, including in-platform instant messaging applications or in-app gift donation features, which the organizers of the crowdfunding initiative may redeem for cash.

The United Nations Counter-Terrorism Committee Executive Directorate noted in 2022 that fundraising loopholes on social media include “super chat” features, such as YouTube’s dollar bill symbol in the chat screen.⁵ Viewers can click on this symbol and use a slider to send a specified dollar amount to the YouTuber, enabling users to donate during livestreams.

VIRTUAL ASSETS

Twelve out of 40 FATF members noted in replies to questionnaires that terrorist groups, such as al-Qaeda and ISIS, have increasingly employed virtual assets in crowdfunding efforts, especially during the past three years.⁶ Services such as tumblers and mixers, which commingle potentially identifiable virtual currencies with others to obscure the trail back to the source, provide an extra measure of anonymity, making tracing the origin and destination of funds more challenging.

However, the use of new payment technologies is not without risk for terrorists. Converting virtual assets to fiat currencies may not always be convenient. In addition, the volatility of virtual assets may introduce additional risks, such as the potential for rapid depreciation, which are not a concern for those who rely on major fiat currencies.

.....
3. U.S. Department of the Treasury, Press Release, “Shutting Down the Terrorist Financial Network December 4, 2001,” December 4, 2001. (<https://home.treasury.gov/news/press-releases/po841>)

4. U.S. Federal Bureau of Investigation, “No Cash for Terror: Convictions Returned in Holy Land Case,” November 25, 2008. (<https://archives.fbi.gov/archives/news/stories/2008/november/hlfi12508>)

5. “CTED’s tech sessions: Highlights on “Threats and opportunities related to new payment technologies and fundraising methods,” *United Nations Security Council – Counter-Terrorism Committee (CTC)*, October 28-29, 2022. (<https://www.un.org/securitycouncil/ctc/news/cted%E2%80%99s-tech-sessions-highlights-%E2%80%99Cthreats-and-opportunities-related-new-payment-technologies-0>)

6. FATF suspended Russia in February 2023, reducing its membership to 39.

DETECTION

Detection of terrorist crowdsourcing requires an understanding of the evolving threat landscape and the actors involved in it. With some forms of terrorism, detection may be triggered by specific jargon or symbolism that may not be familiar to an average user. Terminology, symbols, and even names of groups can evolve, merge, and change over time, making continuing education and monitoring vital to detecting possible terrorist or extremist activity.

According to the Anti-Defamation League, white supremacists in 2017 introduced three extremist-oriented crowdfunding platforms: GoyFundMe, Hatreon, and RootBocks.⁷ In February 2021, a fourth platform, OurFreedomFunding, was established and served as a haven for deplatformed extremists' crowdfunding campaigns in the wake of the January 6 attack on the Capitol in Washington, DC.

The Goyim Defense League (GDL) is a loose network of antisemites who conduct harassment campaigns targeting Jewish people online and in the real world. A GDL connection to crowdfunding campaign would be an immediate source of concern.

Extremist crowdfunding campaigns often allude to the possibility of violence or violent intentions. One example was a campaign hosted on GoyFundMe by a group called the Nationalist Defense Force that described itself as “the only NS [National Socialist] security task force in Weimerica.” The campaign sought to raise funds for “equipment such as, uniforms, (more) shields, pepper spray, helmets, goggles, gas masks, batons, and much more.”

Many aspects of a crowdfunding campaign may point toward the possibility of terrorism or extremism. These include campaign user profiles, the names of campaigns and platforms themselves, and comments posted by donors on crowdfunding sites. All of these may contain language and symbols used by terrorist groups and violent extremists. The online activities of fundraiser organizers may also raise concern.

Fundraisers may also present false or incomplete information about the campaign, its goals, or beneficiaries to mislead donors into supporting terrorist or extremist groups. Furthermore, legitimate funding campaigns are not always easily distinguishable from illegitimate fronts that benefit terrorist groups and causes. Funds for illicit purposes may be commingled with legitimate donations and are not readily detectable by regulatory and/or law enforcement bodies.

The example of Gaza Now, an online media outlet, illustrates the need to conduct research on crowdfunding campaign sponsors. Gaza Now celebrated the recent Hamas attacks in Israel and the kidnapping, torture, and murder of Israelis, according to a recent report by risk and compliance firm Kharon.⁸ The group launched several fundraising campaigns on social media following the attacks and solicited donations in U.S. dollars, euros, and cryptocurrencies. In addition to soliciting donations online, Gaza Now and its founder Mustafa Ayyash have expressed their support of Hamas and its militant leaders on social media. Ayyash in 2017 was arrested by the Austrian authorities for his links to Hamas. He denied the charge and possibly still lives in Austria, managing the Gaza Now account on X (formerly Twitter).⁹

7. “ADL Crowdfunding Report: How Bigots and Extremists Collect and Use Millions in Online Donations,” *Anti-Defamation League*, January 31, 2023. (<https://www.adl.org/resources/report/adl-crowdfunding-report-how-bigots-and-extremists-collect-and-use-millions-online>)

8. “Hamas-Linked Networks Mobilize Crowdfunding Campaigns Following Attacks on Israel,” *Kharon*, October 11, 2023. (<https://brief.kharon.com/updates/hamas-linked-networks-mobilize-crowdfunding-campaigns-following-attacks-on-israel>)

9. @AghaSalarKhan, X, October 31, 2023. (<https://twitter.com/AghaSalarKhan/status/1719442216056144297?s=20>)

INFORMATION SHARING WITH LAW ENFORCEMENT

The operators of most crowdfunding platforms are not regulated by anti-money laundering or counter-terror finance (AML/CFT) regimes. As a result, they do not have reporting obligations or sophisticated monitoring and/or reporting mechanisms like established financial institutions. This lack of effective information-sharing between the public sector and private entities involved in crowdfunding may embolden terrorist groups to continue abusing these platforms.

There is also a need for greater information sharing across jurisdictions. Intelligence services and law enforcement agencies may not have insight into foreign groups and individuals and their links to possible terrorist organizations. That said, coordination and information sharing between jurisdictions is often time-consuming and can delay the investigation process, highlighting the need to develop more efficient mechanisms.

Finally, online fundraising platforms may not require identification verification of the fundraisers and rely on payment processors to perform that function, hampering law enforcement investigations.

FATF HIGHLIGHTS RED FLAGS ASSOCIATED WITH EXPLOITATION OF CROWDFUNDING

The FATF report identifies a number of “red flags” that may reflect the exploitation of crowdfunding platforms, including:

- The use of dedicated payment and crowdfunding platforms that have explicitly declared their willingness to offer services in connection with extremist or terrorist groups;
- The use of crowdfunding platforms with weak project review policies, whose terms of service do not specifically prohibit incitement or support for terrorism, or platforms or intermediaries that host or enable other projects related to violent extremism or terrorism;
- The use of crowdfunding or financial technology platforms, and/or virtual asset wallet addresses associated with individuals or groups linked to terrorism;
- A reliance on donations made through mechanisms used to obscure the donor’s identity or source of funds or that are routed in an overly complex manner;
- The encouragement of donations via anonymity-enhanced cryptocurrencies, such as Monero, Bytecoin, or Zcash; and
- The use of platforms that enable or require payments through unregulated financial institutions.

Legitimate crowdfunding companies should consider campaigns that obscure their purpose, goals, and ultimate beneficiaries as suspicious. In addition to researching organizers’, intermediaries’, and donors’ online rhetoric, platforms should examine the average amount of campaign contributions and determine whether the fundraising goal is unusual or inconsistent with other projects of the same type.

Banks and financial institutions should also ask additional questions and examine those involved in a suspicious campaign, such as:

- Have the organizers or others involved in the crowdfunding campaign been subject to investigations and prosecutions for crimes related to terrorism or violent extremism?

- Do the receipts, amounts sought, or other components of the crowdfunding campaign contain symbols used extensively by known terrorist or violent extremist organizations?
- Does the campaign aim to support a particular group of people, such as relatives of terrorists or foreign fighters, rather than helping a wider community?

Project promoters should also face scrutiny. A closer look may be warranted if the promoter does not appear to be familiar with the project or appears to be a third party unrelated to the fundraiser's purpose. If additional red flags are present, such as the project promoter seeking contributions exclusively in virtual currencies — particularly privacy coins — or if the project promoter closes the crowdfunding page very quickly after the fundraising goal is met, FATF recommends additional due diligence.

Deposits originating from crowdfunding sites followed by speedy structured cash withdrawals should be flagged. Funds received or pooled from multiple accounts and then immediately submitted to crowdfunding campaigns should also result in enhanced due diligence screening.

FATF also recommends closely examining the donors and the geographic risks associated with the crowdfunding campaign. A campaign may represent a more significant jurisdictional risk if the crowdfunding campaign is based in countries (or benefits countries) that do not have strong terrorism financing and/or crowdfunding legislation; countries with poor implementation of FATF standards related to virtual assets, non-profit organizations, or financial transfer services; poor oversight of the crowdfunding industry; or regions where terrorist organizations are known to operate or that are under comprehensive sanctions.

Foundation for Defense of Democracies (FDD)

FDD is a Washington, DC-based nonpartisan research institute focusing on national security and foreign policy.

FDD's Center on Economic and Financial Power (CEFP)

FDD's Center on Economic and Financial Power (CEFP) studies national economic security, with a focus on how the United States can leverage its economic and financial power to achieve its national security objectives. CEFP promotes greater understanding of how the U.S. government can best employ its economic and financial authorities to counter its adversaries.

Nicki Kenyon is associate managing director at DOLFIN. DOLFIN, the Dedicated Online Financial Integrity Network, is a global community dedicated to protecting the financial system's integrity. The content for this article was sourced from the firm's DOLFIN platform — a network of financial integrity professionals that provides insights and developments related to sanctions, export controls, AML/CFT, and other topics of interest to the financial integrity community. **Josh Birenbaum** is deputy director for the Center on Economic and Financial Power at the Foundation for Defense of Democracies.

FDD values diversity of opinion and the independent views of its scholars, fellows, and board members. The views of the authors do not necessarily reflect the views of FDD, its staff, or its advisors.