

EXPERT INSIGHT

Terrorist Use of Crowdfunding

FATF Issues Report about Popular Fundraising Method

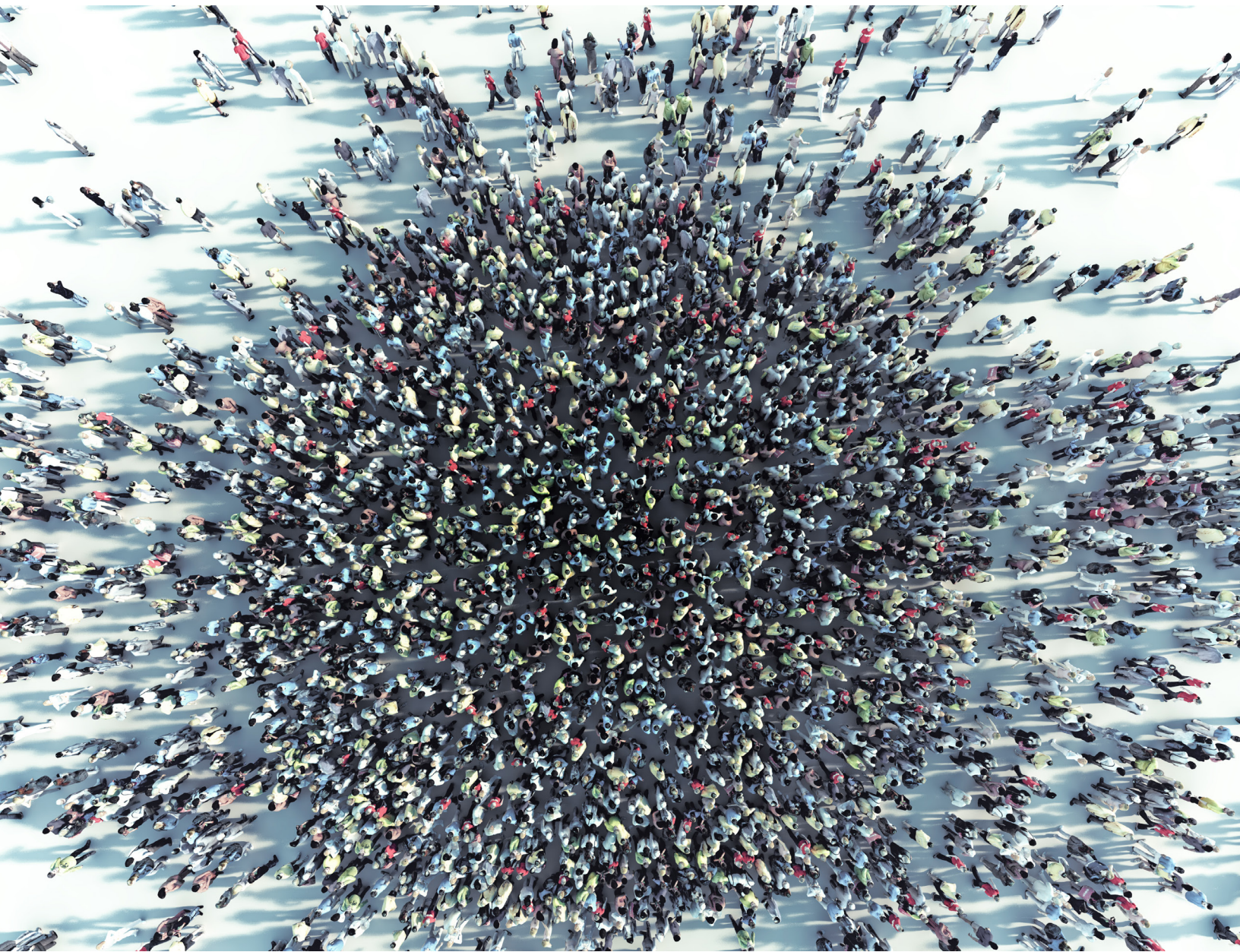


Table of Contents

- 03** Introduction: Terrorist Use of Crowdfunding
- 05** Charities and Nonprofits
- 06** Social Media and Messaging Applications
- 06** Virtual Assets
- 07** Detection
- 09** Information Sharing with Law Enforcement
- 10** Some Red Flags to Consider

Terrorist Use of Crowdfunding

FATF Issues Report about Popular Fundraising Method

The Financial Action Task Force (FATF) in October released its [report](#) on the use of crowdfunding by terrorist and extremist organizations and individuals to raise money for their operations. The nature of crowdfunding, the use of new technologies, and the possible anonymity afforded by crowdfunding platforms can make them attractive as relatively quick and simple means to obtain donations from around the world.

Fundraising through crowdfunding platforms is legal, and numerous worthy causes, startups, small businesses, and nonprofit organizations (NPOs) have used crowdfunding to obtain critical resources for projects, innovations, and charities. However, the diverse landscape of the organizations and entities involved in facilitating these fundraising activities, the lack of transparency, and fragmented data, including about the ultimate recipients, location, true objectives, and origins of donor funds, make these platforms attractive to terrorist organizations and other illicit actors.

Crowdfunding connects supporters with a particular cause and facilitates the transfer of funds between the donor/investor and the ultimate beneficiary. As the global payment and new technologies landscape continue to evolve, so do the mechanisms through which crowdfunding is possible, presenting new challenges and requiring firms, financial institutions, funding facilitators, and law enforcement agencies to keep abreast of rapid changes in the ecosystem and new developments that will facilitate the use crowdfunding platforms by both legal and illicit actors.

FATF this year queried its members about how they regulate crowdfunding and the challenges they face when conducting investigations into the possible misuse of crowdfunding platforms. The FATF report also draws on experiences from the organization's "global network, industry experts, academia, and civil society to build a deeper knowledge of the crowdfunding methods and techniques used by terrorists and to examine best practices in combatting this type of threat."

- Questionnaire responses received in March 2023 from 40 members of the FATF global network indicated that roughly 23 percent of respondent countries do not regulate crowdfunding within the scope of their AML/CFT regimes.
- A further 45 percent of members noted that they regulate crowdfunding activity within the scope of their AML/CFT regimes only when it is offering certain types of services, such as fundraising through the sale of equity or securities.
- An additional 8 percent of jurisdictions regulate donation-based crowdfunding as well as equity or security crowdfunding, but not within the framework of their AML/CFT regimes.
- Only four jurisdictions in FATF's global network regulate both investment and donation-based crowdfunding in the context of their AML/CFT frameworks: France, Monaco, Portugal, and the UK.

The diverse nature of the crowdfunding industry, the multiple crowdfunding models that are used, and the rapidly evolving nature of the industry help explain, at least in part, the different regulatory approaches that exist in different jurisdictions. However, some of the risks and red flags are ubiquitous.



Charities and Nonprofits



Of all the different forms of crowdfunding, donation-based crowdfunding was identified by FATF global network members as most likely to be exploited by terrorists or violent extremists. These illicit actors often exploit humanitarian causes, relying on donors' compassion while hiding behind charitable contributions to divert funds to their operations.

- Fraudulent humanitarian appeals are a typology often observed in crowdfunding for terrorist financing. Individuals may purport to be raising funds for charitable purposes, such as providing social or medical support or building infrastructure projects, but the funding is used to benefit terrorist or violent extremist causes and organizations instead.
- Illicit actors can raise funds for terrorist activities or organizations via social media or formal donation crowdfunding platforms by fraudulently claiming that the support would fund humanitarian aid. The campaign promoters themselves may also be affiliated with a terrorist group.
- Fundraising campaigns can be organized by, or affiliated with, charities that are deemed by national authorities to be operating as fronts for terrorist groups. These organizations may undertake humanitarian relief in addition to funding terrorist activities. The Bush administration in 2001 [designated](#) the Holy Land Foundation (HLF)—the largest Islamic charity in the United States—a terrorist organization and seized its assets. A federal grand jury in 2004 charged the organization and five former officers and employees with providing material support to Hamas. The prosecution asserted, among other things, that HLF distributed funds through charity committees located in the West Bank that paid stipends to the families of Palestinian suicide bombers and Hamas prisoners, and that these charity front organizations served a dual purpose of laundering the money for all of Hamas's activities. The defendants were [convicted](#) in 2008.

Terrorist organizations will mimic financing strategies employed by actual humanitarian organizations, for instance developing promotional videos, setting public funding goals, launching calls to action, and establishing websites or social media pages. However, instead of providing support for humanitarian activities, the funds are collected to provide material support for terrorist group operations or funding to enable travel for foreign fighters. In some cases, only a portion of the funding may be diverted.

NPOs can also unwillingly be exploited by terrorist organizations, especially if they operate in risky geographies, by becoming victims of extortion or skimming. For additional information on the misuse of NPOs by terrorist groups, visit the DOLFIN Library's [Terrorist Financing](#) chapter on the DOLFIN platform.

Social Media and Messaging Applications



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, 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 maximum number of donors.

Some social media sites and messaging apps offer encrypted messaging services to secure conversations and documents, which terrorists and violent extremists can manipulate to share financial data, campaign information, and donation instructions with their networks. The encryption features help avoid detection by competent authorities, and certain messaging applications even have settings that allow messages to only last for a desired time limit, eliminating the possibility of tracking.

Social media sites can also allow donors to donate to causes directly through their platforms, including in-platform instant messaging applications or in-app gift donation features, which can ultimately be redeemed for cash. The UN Counter-Terrorism Committee Executive Directorate [noted](#) in 2022 that fundraising loopholes on social media also include “super chat” features that allow users to make donations during live streams.

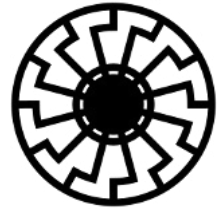
Virtual Assets



Twelve out of 40 delegations noted in replies to their questionnaires that they are seeing more terrorist groups, such as al-Qa'ida and ISIS, use virtual assets in their crowdfunding efforts, with an increase in the detection of these activities during the past three years. Anonymity-enhancing services such as tumblers and mixers provide an extra measure of secrecy, making tracing the origin and destination of funds more challenging.

However, the use of new payment technologies remains challenging for terrorist and extremist groups. Heightened public awareness may bring unwanted attention to these organizations and converting virtual assets to fiat currencies may not always be convenient. In addition, the volatility of the value of virtual assets can introduce additional risks for terrorist groups or violent extremists, who may prefer to rely on more traditional forms of value such as cash.

Detection



Black Sun symbol often used by neo-Nazi groups.

Detection of terrorist and extremist activity requires an understanding of the evolving terrorism threat landscape and the actors involved in it. With some forms of terrorism, detection may even be based on certain terminology or symbolism used, which would not necessarily be apparent to an average reader. 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. 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 anti-Semites who conduct harassment campaigns targeting Jewish people online and in the real world. In June 2021, GDL operated a crowdfunding campaign on GiveSendGo to fund a "Name the Nose" tour, which raised \$398.
- Extremist crowdfunding campaigns often allude to the possibility of violence or violent intentions. For example, a crowdfunding campaign hosted on GoyFundMe by a group called the Nationalist Defense Force, self-described as "the only NS [National Socialist] security task force in Weimerica" on their profile, was raising funds for "equipment such as, uniforms, (more) shields, pepper spray, helmets, goggles, gas masks, batons, and much more."

Unwitting donors can contribute to a crowdfunding campaign without knowledge of its illicit purpose. Fundraisers may also present false or incomplete campaign information, goals, or beneficiaries to mislead donors into contributing to a fraudulent campaign that will ultimately end up in the hands of terrorist or extremist groups. Terrorists may exploit donors' sympathies (e.g., for victims of natural or humanitarian disasters) and manipulate the general public's lack of awareness about terrorist organizations to procure donations.

Examining fundraising campaign user profiles, the names of campaigns and platforms themselves, as well as comments posted by donors on crowdfunding sites for language and symbols often used by terrorist groups and violent extremists can provide insight into the nature of the campaign and its organizers. Monitoring the online activities of fundraiser organizers can also inform decision making.

- Online media outlet 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. The group launched several fundraising campaigns on social media following the attacks and solicited donations in US 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).



Information Sharing with Law Enforcement

Lack of effective information sharing mechanisms between the public sector and private entities involved in crowdfunding can embolden terrorist groups to continue abusing these platforms. Most intermediary organizations facilitating donation-based crowdfunding are not regulated by AML/CFT regimes and do not have reporting obligations or sophisticated monitoring and/or reporting mechanisms like established financial institutions.

- The relative complexity and fragmentation of crowdfunding operations creates an opaque context for reporting entities to conduct due diligence. For example, determining whether the funds received into an account were from legitimate donors and consistent with similar campaigns can be challenging.
- Tracing potentially suspicious crowdfunding transactions may also be challenging for reporting entities, given that payment references for some platforms (mostly social media platforms) do not always identify accounts where the payment was made.
- Many crowdfunding campaigns attract small-scale, anonymous transactions, which are difficult to detect among the vast, largely legitimate, crowdfunding ecosystem and prevent effective reporting of suspicious transactions.

The complexity of the crowdfunding payment landscape increases the challenges for investigative and prosecution authorities. Crowdfunding transactions can involve several actors and intermediaries, such as social media platforms, payment processors, virtual currency mixers, and financial institutions. Various digital payment methods are often used, allowing users to move funds quickly, and allowing the use of pseudonyms or anonymous transactions. Digital fundraising technology is complex and requires specialist expertise to investigate and track suspicious transactions.








Intelligence services and law enforcement agencies may not have insight into foreign groups and individuals and their links to possible terrorist or extremist organizations, making information-sharing among partners and allies critical to detection. However, coordination and information sharing between jurisdictions may be time-consuming and delay the investigation process. Where crowdfunding entities are not subject to regulation, challenges obtaining information can arise.

Legitimate funding campaigns are not always easily distinguishable from fronts that can benefit terrorist groups and causes. Funds for illicit purposes can be comingled with legitimate donations and are not readily detectable by regulatory and/or law enforcement bodies. Financial institutions with reporting obligations may not be aware that specific customer activity is linked to crowdfunding platforms or social media activity, impacting law enforcement and regulators' awareness of this activity.




In addition, online fundraising platforms may not require identification verification of the fundraisers and rely on payment processors to perform that function, posing difficulties in obtaining the information of the beneficiaries of fundraising activities and hampering law enforcement investigations.

Some Red Flags to Consider

The FATF report identifies red flags that may highlight suspicious activity related to terrorist and extremist fundraising through crowdfunding platforms.

-  Projects that are promoted through crowdfunding platforms that have weak project review policies or whose terms of service do not specifically prohibit content that incites and supports terrorism or violent extremism.
-  The crowdfunding, FinTech platforms, and/or virtual asset wallet addresses are known to be used by individuals or groups associated with terrorism and/or violent extremism.
-  Donations appear to be made through mechanisms used to obscure identity or source of funds or are routed in a way that is overly complex.
-  The crowdfunding platform or intermediary organization hosts or enables other projects related to violent extremism or radicalism.
-  The use of dedicated payment and crowdfunding platforms that have explicitly declared their willingness to offer services in connection with extremist or terrorist groups.
-  Platforms that enable or require payments through unregulated financial institutions.
-  The entity encourages methods of donation that try to hide transaction information using anonymity enhanced cryptocurrencies, such as Monero, Bytecoin, or Zcash.

Legitimate crowdfunding companies should consider campaigns that obscure the purpose, goals, and ultimate beneficiaries of the campaign as suspicious. In addition to researching organizers', intermediaries', and donors' online rhetoric, platforms should also examine the average amount of campaign contributions and determine whether the fundraising goal is unusual or inconsistent with other projects of the same kind. Banks and financial institutions should also ask additional questions and examine those involved in the campaign.

-  Have the organizers of 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 and 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, according to FATF. If the project promoter does not appear to be familiar with the project or appears to be a third party unrelated to the purpose of the fundraiser, a closer look may be warranted. 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 or received or pooled from multiple accounts and then immediately submitted to crowdfunding campaigns should result in enhanced due diligence.

FATF also recommends closely examining the donors and the geographic risks associated with the crowdfunding campaign. 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 and poor oversight of the crowdfunding industry, or geographic zones where terrorist organizations are known to operate or that are under comprehensive sanctions, the crowdfunding campaign may represent a more significant jurisdictional risk.

Close monitoring of the geographic origins of donations and their destination, particularly to and from countries where terrorist organizations are known to operate or that are a high risk of terrorist financing should be standard for platforms and intermediaries.

DOLFIN's [database](#) of red flags can help financial institutions, payment processors, social media and crowdfunding platforms, and messaging applications identify risk indicators related to terrorist and extremist financing. The database is regularly updated, as new methodologies are identified by regulators, law enforcement, and international organizations.