



FinCEN

ALERT

FIN-2026-Alert008

October 15, 2026

FinCEN Alert to Counter Iranian Abuse of Religious Charity Networks

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this Alert by including the key term “**FIN-2026-IRANCHARITYABUSE**” in SAR field 2 (Filing Institution Note to FinCEN) and the narrative.

The U.S. Department of the Treasury’s (Treasury) Financial Crimes Enforcement Network (FinCEN) is issuing this Alert to assist financial institutions¹ in identifying and reporting potential Iranian abuse of religious charity networks, including diversion of religious tithes or *khums*. This Alert supports Treasury’s efforts as part of Operation Economic Outcast targeting the Iran and its financial enablers, including the Islamic Revolutionary Guard Corps (IRGC).²

The information contained in this Alert is derived from analysis of Bank Secrecy Act data, as well as open-source reporting and law enforcement information.

The Iranian regime has a long history of abusing religious-affiliated institutions and charitable organizations to line the pockets of its elites, fund repression within Iran, and support violence abroad. For example, in 2020, Treasury’s Office of Foreign Assets Control (OFAC) designated the Islamic Revolution Mostazafan Foundation (Bonyad Mostazafan).³ As Treasury explained at the time, “[w]hile Bonyad Mostazafan is ostensibly a charitable organization charged with providing benefits to the poor and oppressed, its holdings are expropriated from the Iranian people and are used by [Iran’s Supreme Leader] to enrich his office, reward his political allies, and persecute the regime’s enemies.”⁴ In addition, in 2020, OFAC designated the Reconstruction Organization of the Holy Shrines in Iraq (ROHSI), an ostensibly religious institution based in Iran and Iraq that is in reality controlled by the IRGC-Qods Force.⁵ ROHSI transferred millions of dollars to an Iraq-based

1. See 31 U.S.C. 5312(a)(2); 31 C.F.R. 1010.100(t).

2. See Treasury, Press Release, “[Treasury Launches Unprecedented Campaign Against Iranian Regime on Economic D-Day](#)” (Aug. 24, 2026).

3. See Treasury, Press Release, “[Treasury Targets Vast Supreme Leader Patronage Network and Iran’s Minister of Intelligence](#)” (Nov. 18, 2020). “Bonyads are opaque, quasi-official organizations controlled by current and former government officials and clerics that report directly to the Supreme Leader. Bonyads receive benefits from the Iranian government, including tax exemptions, but are not required to have their budgets publicly approved. They account for a significant portion of Iran’s non-petroleum economy, with the [Islamic Revolution Mostazafan] Foundation itself estimated to account for over one percent of Iran’s gross domestic product.” *Id.*

4. *Id.*

5. See Treasury, Press Release, “[Treasury Designates Vast Network of IRGC-QF Officials and Front Companies in Iraq, Iran](#)” (“Mar. 2020 Treasury Press Release”) (Mar. 26, 2020). For more information about IRGC financing, see FinCEN, FIN-2026-Alert002, “[FinCEN Alert on the Use of Front Companies, Financial Facilitators, and Digital Asset Infrastructure by Iran’s Islamic Revolutionary Guard Corps to Evade Sanctions and Launder Proceeds](#)” (May 11, 2025).

IRGC-controlled company that served as a base for Iranian intelligence activities in Iraq as well as the shipment of weapons and ammunition to Iranian-backed terrorist militia groups.⁶

The Iranian regime similarly strives to co-opt *khums* payments—the practice of donating a fifth of one’s surplus annual income to religious institutions to fund social and religious programs⁷ — from the global Shi’a community to further its destabilizing activities. *Khums* payments fulfill an important role in Shi’a communities. However, in some cases, organizations that collect these payments do so on behalf of prominent Iranian ayatollahs with ties to the regime or on behalf of the Supreme Leader himself. These entities may use informal financial channels, such as the hawala system⁸ and cash couriers, to remit the funds to Iran or to Iran-linked actors. For example, in 2024, Muzzamil Zaidi and Asim Mujtaba Naqvi pleaded guilty for their roles in an illicit scheme to collect tens of thousands of dollars, including *khums* payments, from the United States for transfer to Iran, including in the name of former Supreme Leader Khamenei, in violation of U.S. economic sanctions laws.⁹ According to the Department of Justice, “Zaidi and Naqvi enlisted friends, family members, and other associates to carry the cash out of the United States, in amounts of less than \$10,000 in order to avoid law enforcement scrutiny. One transfer of dollars to Iran involved a group of 25 travelers going on a religious pilgrimage in Iraq,” who subsequently hand-carried those U.S. dollars to Iran.

Red Flag Indicators for Iranian Abuse of Religious Charities

FinCEN has identified the following red flag indicators to help financial institutions detect, prevent, and report suspicious activity potentially involving Iran’s abuse of religious charity networks, including when Iran’s direct involvement is not readily identifiable in transaction details. These red flags are in addition to the red flags pertaining to charity and nonprofit organization (NPO) abuse by Iran and its proxies identified in prior FinCEN products, including in its *Advisory to Financial Institutions to Counter the Financing of Iran-Backed Terrorist Organizations*¹⁰ and in its *Alert to Financial Institutions to Counter Financing to Hamas and its Terrorist Activities*.¹¹ As no single red flag is determinative of illicit or suspicious activity, financial institutions should consider the totality of available facts and circumstances, such as a customer’s historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple red flags before determining that a behavior or transaction is suspicious. Financial institutions are also encouraged to submit notifications to OFAC when they identify potential sanctions violations through the [Disclosure Portal](#), while continuing to submit Suspicious Activity Reports (SARs) as appropriate.

6. See Mar. 2020 Treasury Press Release, *supra* note 5.

7. See Elvire Corboz, Cambridge University Press, “[Part II - Charitable Politics: Benevolent Patrons, Beneficiaries and the State](#)” (Aug. 5, 2016).

8. The Financial Action Task Force (FATF) defines hawalas and other similar service providers (HOSSPs) as “money transmitters, particularly with ties to specific geographic regions or ethnic communities, which arrange for [the] transfer and receipt of funds or equivalent value and settle through trade, cash, and net settlement over a long period of time.” FATF, “[The Role of Hawala and Other Similar Service Providers in ML/TF](#)” (Oct. 2013), at p. 9.

9. Department of Justice, Press Release, “[Scheme to Transfer Money to Iran Results in Guilty Pleas](#)” (May 1, 2024).

10. FinCEN, FIN-2024-A001, “[FinCEN Advisory to Financial Institutions to Counter the Financing of Iran-Backed Terrorist Organizations](#)” (May 8, 2024).

11. FinCEN, FIN-2023-Alert006, “[FinCEN Alerts Financial Institutions to Hamas’s Terrorist Financing](#)” (Oct. 20, 2023).

- 1 A customer that is a charitable organization or NPO solicits donations but does not appear to provide any charitable services or openly supports the Iranian regime or its terrorist proxies, such as in fundraising appeals or on social media.
- 2 A customer that is a charitable organization or NPO receives large donations from an unknown source over a short period of time and then sends significant wire transfers or checks to other charitable organizations or NPOs.
- 3 A customer that is a charitable organization or NPO, or an employee, officer, or contractor of a charitable organization or NPO, engages in a pattern of behavior suggesting efforts to evade the Currency Transaction Report (CTR) reporting requirement (*e.g.*, alters or cancels a transaction when advised a CTR would be filed or engages in structuring with multiple cash transactions in amounts below \$10,000), as well as avoiding recordkeeping requirements.¹²
- 4 A customer receives transfers from a charitable organization or NPO with which the customer has no clear business relationship and then proceeds to withdraw the funds in cash or remit them onward.

FinCEN continues to emphasize that legitimate charities should have access to financial services and can transmit funds through legitimate and transparent channels. As set out in the Joint Fact Sheet on Bank Secrecy Act Due Diligence Requirements for Charities and Non-Profit Organizations, banks are reminded to apply a risk-based approach to customer due diligence (CDD) requirements when developing the risk profiles of charities and other non-profit customers. The application of a risk-based approach is consistent with existing CDD and other Bank Secrecy Act/AML compliance requirements.¹³

FinCEN requests that financial institutions reference this Alert by including the existing key term “FIN-2026-IRANCHARITYABUSE” in SAR field 2 (Filing Institutions Note to FinCEN).

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, counter money laundering and the financing of terrorism, and promote national security through strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.

Updates, questions, or comments regarding the contents of this Alert should be addressed to the FinCEN Regulatory Support Section by submitting an inquiry at www.fincen.gov/contact.

12. See generally 31 C.F.R. §§ 1010.100(xx), 1010.310-314, 1010.410; see also Federal Reserve, FDIC, FinCEN, NCUA, OCC, “[Frequently Asked Questions Regarding Suspicious Activity Reporting Requirements](#)” (Oct. 9, 2025) (noting that “[t]he mere presence of a transaction or series of transactions by or on behalf of the same person at or near the \$10,000 CTR threshold is not information sufficient to require the filing of a SAR” and that “[f]inancial institutions are only required to file a SAR if the institution knows, suspects, or has reason to suspect that the transaction or series of transactions are designed to evade CTR reporting requirements” (citations and emphasis omitted)).

13. See FinCEN, Federal Reserve, FDIC, NCUA, and OCC, “[Joint Fact Sheet on Bank Secrecy Act Due Diligence Requirements for Charities and Non-Profit Organizations](#)” (Nov. 19, 2020).