FinCEN NOTICE

FIN-2026-NTC2 October 30, 2026

FinCEN Notice on the Use of Charities and Non-Profit Organizations for Illicit Activity

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this Notice by including the key term "**FIN2026NPO**" 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 Notice to assist financial institutions[1] in identifying and reporting suspicious activity involving the exploitation of domestic and international charities and non-profit organizations (collectively, NPOs) for illicit activity.

NPOs deliver essential aid, services, and assistance to vulnerable populations and perform other important services for the public good. NPOs are, however, vulnerable to abuse by individuals taking advantage of the public trust placed in NPOs and exploiting NPOs' fundraising capabilities to facilitate terrorist financing, fraud, and other illicit activity. Through schemes abusing NPOs, bad actors can funnel funds to terrorists, divert funds from government programs, and steal money intended for charitable causes. The Trump Administration is focused on supporting access to financial services for legitimate NPOs and NPO employees while preventing NPO abuse and will use its authorities to prevent terrorists from using NPOs to fund their operations.[2]

In general, the vast majority of U.S.-based NPOs present a low risk of terrorist financing and other illicit activities, and the U.S. government does not view the NPO sector as a whole as presenting a uniform or unacceptably high risk.[3] FinCEN encourages financial institutions interacting with

1. *See* 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 1010.100(t).
2. *See, e.g.*, Treasury, Press Release, "Treasury Disrupts Muslim Brotherhood and Hamas Financial Networks" (July 23, 2026); Treasury, Press Release, "Treasury Continues to Disrupt Hamas' Sham Charity Network as the Group Refuses to Disarm" (Mar. 12, 2026) [hereinafter "March 2026 OFAC Action"]; Treasury, Press Release, "Treasury Takes Action Against Violent Far-Left Terrorist Networks" (Aug. 26, 2026) [hereinafter "August 2026 OFAC Action"] (designating certain terrorist networks); Treasury, "2026 National Terrorist Financing Risk Assessment" (Mar. 2026), at 20 [hereinafter "2026 NTFRA"]; Department of State, Press Release, "Designations of Antifa Ost and Three Other Violent Antifa Groups" (Nov. 13, 2025); *see also* Treasury, Press Release, "Secretary Bessent Delivers Remarks Before the Ministerial on the Resurgence of Political Terrorism" (July 16, 2026).
3. FinCEN, Board of Governors of the Federal Reserve System (Federal Reserve), Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), and Office of the Comptroller of the Currency (OCC), "Joint Fact Sheet on Bank Secrecy Act Due Diligence Requirements for Charities and Non-Profit Organizations" (Nov. 19, 2020) [hereinafter "NPO Fact Sheet"]; *see also* Financial Action Task Force, "Combating the Terrorist Financing Abuse of Non-Profit Organisations" (Nov. 2023) (emphasizing the importance of "effective implementation of a risk-based approach" with respect to the NPO sector).

NPOs to apply a risk-based approach and determine whether they can effectively mitigate potential vulnerabilities relating to NPOs by evaluating each NPO individually.[4]

This Notice aligns with FinCEN's Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) National Priorities of Fraud, Terrorist Financing, and Corruption.[5] Preventing abuse in the NPO sector also furthers the Administration's efforts to counter fraud, including President Trump's E.O. 14249, *Protecting America's Bank Account Against Fraud, Waste, and Abuse*.[6]

The information in this Notice is derived from Bank Secrecy Act (BSA) data, open-source reporting, and information provided by law enforcement.

NPO Background

As of September 2026, there were approximately 1.96 million registered "exempt organizations" in the United States, which includes "[o]rganizations organized and operated exclusively for religious, charitable, scientific, testing for public safety, literary, educational, or other specified purposes."[7] One study estimates that contributions to U.S. charities in 2025 were approximately $617.2 billion.[8] The NPO sector accounted for nearly 10% of U.S. private sector employment.[9]

NPOs are subject to federal and state reporting requirements and regulatory oversight.[10] Among other things, NPOs generally report information annually on IRS Form 990 regarding their stated mission, programs, finances, donors, activities, and funds sent and used abroad.[11] Similarly, most states require NPOs to register before they solicit the state's residents for contributions.[12] In addition to legal obligations, NPOs often follow voluntary self-regulatory standards to improve governance, management, and operational practices, as well as internal controls required by funders and others.[13]

4. This Notice should be read in conjunction with Executive Order (E.O.) 14331, *Guaranteeing Fair Banking for All Americans*, which furthers the policy of ensuring that banking decisions are made on the basis of individualized, objective, and risk-based analyses and that no American is denied access to financial services because of constitutionally protected or statutorily protected beliefs, affiliations, or political views. The White House, "Guaranteeing Fair Banking for All Americans," 90 Fed. Reg. 38,925 (Aug. 12, 2025) [hereinafter "Fair Banking E.O."].
5. *See* FinCEN, "AML/CFT National Priorities" (June 30, 2021).
6. *See* The White House, "Protecting America's Bank Account Against Fraud, Waste, and Abuse," 90 Fed. Reg. 14,011 (Mar. 28, 2025).
7. *See* Internal Revenue Service (IRS), "Exempt Organizations Business Master File Extract (EO BMF)" (Sept. 8, 2026); IRS, "Exempt Organization Types" (June 28, 2026).
8. Indiana University Lilly Family School of Philanthropy, "Giving USA 2026: The Annual Report on Philanthropy for the Year 2025" (June 23, 2026).
9. Private sector employment information as of 2022. *See* Bureau of Labor Statistics, U.S. Department of Labor, "Nonprofits Accounted for 12.8 Million Jobs, 9.9 Percent of Private-Sector Employment, in 2022" (Aug. 16, 2024).
10. *See, e.g.*, IRS, "Life Cycle of a Public Charity" (July 3, 2026); IRS, "State Links" (June 28, 2026); *see also* NPO Fact Sheet, *supra* note 3, at 3.
11. *See* IRS, "Annual Filing and Forms" (June 28, 2026); *see also* Treasury, Press Release, "Treasury Announces Form 990 Transparency Initiative to Expose Hidden Funding and Strengthen Oversight" (Apr. 23, 2026); IRS, "Instructions for Form 990 Return of Organization Exempt from Income Tax" (2025).
12. *See* IRS, "Before Applying for Tax-Exempt Status" (June 27, 2026); IRS, "Charitable Solicitation - Initial State Registration" (June 28, 2026).
13. *See* 2026 NTFRA, *supra* note 2, at 20–21; *see also* Treasury, "2018 National Terrorist Financing Risk Assessment" (Dec. 20, 2018), at 24.

NPOs that meet the requirements of Internal Revenue Code section 501(c)(3) may apply to the IRS for tax-exempt status, which, if granted, exempts the organization from federal income tax as a "charitable organization."[14] Additionally, contributions made to charitable organizations by individuals and corporations may be deductible under Internal Revenue Code section 170.[15]

Schemes Associated with NPO Abuse

NPO abuse schemes fall into three general categories: (1) sham charities; (2) NPO fraud; and (3) NPO embezzlement. However, in some cases these schemes may exhibit characteristics of multiple categories. Moreover, entities involved in sham charity or NPO fraud schemes may present themselves as NPOs but may not actually be organized, registered, or recognized as tax-exempt under applicable federal or state law.

Sham Charity Schemes

In sham charity schemes, bad actors publicly advertise an NPO as serving a legitimate purpose but, in reality, use the NPO for illicit activity. For example, an entity may claim to raise funds for humanitarian goals while actually sending funds to—and coordinating with—a terrorist organization.[16] The sham charity's management will be complicit in furthering the illicit activities of the NPO, for example, by concealing illicit activities and coordinating with the ultimate illicit recipient of the funds.[17] In certain cases, donors may be aware of the sham charity's true objectives and knowingly use the entity as a mechanism to send funds to further the illicit activities.[18] In other cases, donors may contribute to a sham charity based on its purported legitimate activities, with no knowledge of the NPO's illicit activities.[19] Bad actors may use sham charities to further terrorist activities, as well as for other illicit purposes, such as purchasing political favors.[20]

Treasury has previously released information on NPO risks related to the funding of terrorist activity, in both the United States and abroad, including by Hamas[21] and other Iran-backed terrorist

14. *See* IRS, "Application Process" (June 28, 2026).
15. *See* IRS, "Exemption Requirements - 501(c)(3) Organizations" (June 28, 2026).
16. *See, e.g.*, Department of State, "Country Reports on Terrorism 2024" (May 1, 2026) (listing foreign terrorist organizations that raise funds through NPOs); Treasury, Press Release, "United States and Canada Target Key International Fundraiser for Foreign Terrorist Organization PFLP" (Oct. 15, 2024).
17. *See, e.g.*, March 2026 OFAC Action, *supra* note 2.
18. *See, e.g.*, Treasury, Press Release, "Treasury Disrupts Sham Overseas Charity Networks Funding Hamas and the PFLP" (June 10, 2025) [hereinafter "June 2025 OFAC Action"]; Treasury, Press Release, "Treasury Targets Additional Sources of Support and Financing to Hamas" (Oct. 27, 2023) (noting that the "Iranian Bonyad Shahid, also known as the Martyrs Foundation, which was designated in 2007, provides millions of dollars through the Gaza-based and Palestinian Islamic Jihad (PIJ)-affiliated Al-Ansar Charity Association (Al-Ansar) for the families of terrorists affiliated with Hamas and PIJ").
19. *See* June 2025 OFAC Action, *supra* note 18; Treasury, Press Release, "Treasury Exposes and Disrupts Hamas's Covert Support Network" (Jan. 21, 2026) [hereinafter "January 2026 OFAC Action"].
20. *See* Department of Justice (DOJ), Press Release, "Mobile Telesystems PJSC and Its Uzbek Subsidiary Enter into Resolutions of $850 Million with the Department of Justice for Paying Bribes in Uzbekistan" (Mar. 7, 2019).
21. *See* FinCEN, FIN-2023-Alert006, "FinCEN Alert to Financial Institutions to Counter Financing to Hamas and its Terrorist Activities" (Oct. 20, 2023) [hereinafter "Hamas Alert"].

organizations.[22] As noted in FinCEN's 2023 Alert, Hamas uses sham charities that purport to provide humanitarian assistance but, in fact, primarily or exclusively funnel money to terrorist organizations.[23] FinCEN's 2024 Advisory further describes how Hamas has sought digital asset contributions in donation drives since at least 2019[24] and has historically used virtual asset service providers in an attempt to safeguard the anonymity of its donors.[25] The 2024 Advisory also explains how Hamas exploits crowdfunding and social media platforms to raise funds under the guise of humanitarian or charitable causes worldwide.[26] According to analysis of BSA data, these donations are often placed in bank accounts in countries such as Lebanon, Qatar, and Türkiye and are then accessed by individuals operating in the Gaza Strip. Similarly, Treasury's Office of Foreign Assets Control (OFAC) has designated Iranian charitable organizations that, rather than providing humanitarian assistance or welfare services, act as conglomerates in key sectors of the Iranian economy and are used by the country's leadership to enrich itself, reward political allies, and persecute enemies.[27]

Case Studies: Terrorist Financing Sham Charity Schemes

On October 7, 2024,[28] June 10, 2025,[29] January 21, 2026,[30] March 12, 2026,[31] and August 26, 2026,[32] OFAC designated NPOs and related individuals responsible for funding and supporting Hamas, the Popular Front for the Liberation of Palestine (PFLP), and the Muslim Brotherhood. The designated parties exhibit various sham charity typologies.

In one case, a terrorist organization directly controlled the charity or assigned its members to work for the NPO. OFAC noted that Gaza-based charity Al Weam Charitable Society (Al Weam) is clandestinely controlled by Hamas and fully integrated into Hamas's military wing. This secrecy has allowed Al Weam to raise funds and implement projects funded by international donors, many of whom are unaware of the organization's ties to Hamas. Al Weam has also employed Hamas members throughout the organization, including its Chairman of the Board of Directors, Muhammad Sami Muhammad Abu Marei, a Hamas military operative who used Al Weam to fundraise on behalf of Hamas.[33]

22. *See* FinCEN, FIN-2024-A001, "FinCEN Advisory to Financial Institutions to Counter the Financing of Iran-Backed Terrorist Organizations" (May 8, 2024) [hereinafter "Iran-Backed Terrorist Organizations Advisory"].
23. *See* Hamas Alert, *supra* note 21.
24. *See* Iran-Backed Terrorist Organizations Advisory, *supra* note 22; Congressional Research Service, "Terrorist Financing: Hamas and Cryptocurrency Fundraising" (Dec. 9, 2024), at 1; *see also* DOJ, Press Release, "San Diego Resident Charged with Conspiring to Provide Material Support to Hamas" (June 17, 2026); DOJ, Press Release, "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns" (Aug. 13, 2020).
25. *See* Iran-Backed Terrorist Organizations Advisory, *supra* note 22.
26. *See id*.
27. *See* Treasury, Press Release, "Treasury Targets Vast Supreme Leader Patronage Network and Iran's Minister of Intelligence" (Nov. 18, 2020) ("While the Supreme Leader enriches himself and his allies, the Foundation's primary mission to care for the poor has become a secondary objective. According to the Foundation's previous president, in past years as little as seven percent of the Foundation's profit has been spent on projects aimed at reducing poverty."); Treasury, Press Release, "Treasury Sanctions Vast Financial Network Supporting Iranian Paramilitary Force That Recruits and Trains Child Soldiers" (Oct. 16, 2018).
28. *See* Treasury, Press Release, "Treasury Targets Significant International Hamas Fundraising Network" (Oct. 7, 2024).
29. *See* June 2025 OFAC Action, *supra* note 18.
30. *See* January 2026 OFAC Action, *supra* note 19.
31. *See* March 2026 OFAC Action, *supra* note 2.
32. *See* August 2026 OFAC Action, *supra* note 2.
33. *See* June 2025 OFAC Action, *supra* note 18.

In the case of the Gaza-based organizations Waed Society Gaza (Waed Society), Al-Nur Society Gaza, Qawafil Society Gaza, Al-Falah Society Gaza, Merciful Hands Gaza, and Al-Salameh Society Gaza (Al-Salameh), members of Hamas's internal security forces are formally assigned to work in these charities, specifically the Waed Society and Al-Salameh. Documentary evidence captured from Hamas also shows that Hamas provides its fighters with detailed instructions on navigating its internal bureaucracy, including how to formally request specific projects and services from affiliated organizations.[34]

In another case, an NPO diverted funds to a terrorist organization. El Baraka Association for Charitable and Humanitarian Work (El Baraka), based in Algeria, diverted funds intended for humanitarian causes to fund Hamas. As President of El Baraka, Ahmed Brahimi worked to ensure that funds raised by the NPO, including some from unwitting donors who thought they were helping Palestinian civilians, were instead diverted to Hamas.[35]

In another scheme, an NPO purported to raise funds for a legitimate cause but supported terrorist activity, including by receiving funds from other sanctioned entities. Addameer Prisoner Support and Human Rights Association (Addameer), based in the West Bank, purported to represent the interests of Palestinian prisoners. However, like the Samidoun Palestinian Prisoner Solidarity Network (Samidoun) that OFAC designated on October 15, 2024, along with one of its leaders, Khaled Barakat (Barakat), Addameer has long supported and is affiliated with the PFLP. Additionally, in the spring of 2022, Barakat coordinated with the PFLP to send funds to Addameer and to arrange meetings between Addameer and Samidoun.[36]

In a further instance, an NPO, in addition to providing support, served as a hub for a terrorist organization. Hayat Yolu is a Türkiye-based NPO that has provided significant material support to Hamas. Additionally, it has been identified as an operational headquarters and a banking and financial hub for the Muslim Brotherhood.[37]

NPO Fraud Schemes

In NPO fraud schemes, as in sham charity schemes, bad actors operate an NPO to further illicit activities. However, in NPO fraud schemes, criminals misuse the NPOs to enrich themselves rather than support an illicit cause or activity. For example, an NPO may advertise a charitable purpose but provide few, if any, charitable services, instead diverting funds to support the lifestyle of its leadership or closely connected individuals. In these schemes, NPO leadership is complicit in furthering the NPO's illicit goal, though not all employees are necessarily complicit. Entities in NPO fraud schemes may solicit donations from the public through traditional appeals and fundraising initiatives, grants from foundations, social media, or crowdfunding. Donors to these NPOs are typically unaware of the true use of their donations—they are victims of the NPO fraud scheme. NPOs may also be the recipients of federal and state funds designed to provide a public

34. *See* January 2026 OFAC Action, *supra* note 19.
35. *See* June 2025 OFAC Action, *supra* note 18.
36. *Id.*
37. *See* March 2026 OFAC Action, *supra* note 2.

benefit, which the NPOs instead redirect to enrich their management and others. Because NPOs in these schemes may provide few or no services, they may have a limited physical and online presence. For example, an NPO may list its official address as a post office box, a commercial mail receiving agency, or a location inconsistent with the expectation for an NPO, such as a residential address or commercial address connected with an unrelated business. Similarly, because these NPOs may have limited operations, they may have no employees other than an NPO manager and no operational expenditures.

Fraudulently Obtained or Misappropriated Donations

Entities in NPO fraud schemes may solicit funds directly from the public, at times in response to natural disasters or mass casualty events.[38] The Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) reported that, in 2024, it received over 4,500 complaints related to fraudulent charities, crowdfunding accounts, and disaster relief campaigns, resulting in approximately $96 million in losses.[39] Entities in NPO fraud schemes may raise funds from different types of unwitting donors; often, fraudsters target older adults when soliciting donations.[40] While many fraudulent schemes with a charity nexus operate through NPOs or use NPOs to receive money, in certain cases, bad actors may receive the illicit proceeds directly as individuals.[41]

The use of advertisements, social media, and crowdfunding platforms allows NPOs engaged in fraud to connect with and raise funds from a diverse group of donors. In other cases, an NPO may raise money by targeting legitimate charitable organizations or religious communities. Fraudsters may also create a web of NPOs purportedly addressing a variety of charitable causes (including by using names that are similar to existing, legitimate NPOs) operating from the same addresses or using the same accounts.[42]

38. *See* FinCEN, FIN-2017-A007, "Advisory to Financial Institutions Regarding Disaster-Related Fraud" (Oct. 31, 2017); FBI, "Charity and Disaster Fraud" (last accessed Aug. 27, 2026); Federal Communications Commission, "After Storms, Watch Out for Scams" (Nov. 20, 2025).
39. *See* FBI, I-011625-PSA, "Beware of Charitable Fraud Related to Mass Casualty and Disaster Events" (Jan. 16, 2025); *see also* Federal Trade Commission, "Before Giving to a Charity" (Sept. 2025). In 2025, IC3 began to track charity fraud as a separate category of fraud and reported 662 complaints connected to almost $8 million in losses. FBI, "2025 Internet Crime Report" (Apr. 6, 2026).
40. *See* OCC, "Elder Financial Exploitation" (Jan. 14, 2025); *see also* FinCEN, FIN-2022-A002, "Advisory on Elder Financial Exploitation" (June 15, 2022); FinCEN, Consumer Financial Protection Bureau, Federal Reserve, FDIC, NCUA, OCC, State Financial Regulators, "Interagency Statement on Elder Financial Exploitation" (Dec. 4, 2024; updated June 2026).
41. *See, e.g.*, DOJ, U.S. Attorney's Office for the District of New Jersey, Press Release, "Philadelphia Man Sentenced to Three Years of Probation for Role in Scheme to Launder Money, Defraud Internet Donors" (Oct. 3, 2022).
42. *See, e.g.*, DOJ, U.S. Attorney's Office for the District of Columbia, Press Release, "Maryland Man Found Guilty in Scheme that Bilked Benevolent Donors of Charitable Contributions" (May 15, 2023) (describing how two individuals "creat[ed] fake charities and register[ed] those entities with the D.C. Department of Consumer and Regulatory Affairs and then present[ed] them as legitimate charities. Examples included the 'Disabled and Paralyzed Veterans Fund,' the 'National Breast Cancer Awareness Fund,' and the 'Children's Leukemia of America Fund'"); Michigan Department of Attorney General, Press Release, "Fraudulent Organizations Posing as Charitable Nonprofits Ordered Dissolved" (July 1, 2021) (noting that "[t]he entities have names similar to those of legitimate nonprofits, like the American Cancer Society, American Cancer Foundation, United Way and the American Red Cross, but appear to serve no charitable or commercial purpose").

Misappropriated Government Funding

In some cases, entities in NPO fraud schemes exploit government funding. These NPOs may receive reimbursements or grants from the U.S., state, or local governments for the purported provision of social services (including medical, childcare, homelessness, and educational services) and then use various schemes to misappropriate or divert the funding.[43]

Funding for NPOs purportedly administering government benefits can come from a variety of governmental sources, and funds credited to NPO accounts may originate from different government entities, partners, or intermediaries. Funds may come directly from the Federal Government (for example, through a grant by a Federal department), from a state agency administering Federal funds (as in the case of the U.S. Department of Agriculture's Child and Adult Care Food Program and Summer Food Service Program), through special-purpose state and local authorities, or even from other NPOs receiving government funding. Fraudsters may, in certain cases, conduct multiple concurrent NPO fraud schemes that take advantage of several different sources of government funding.

In certain cases, the NPOs engaged in the fraud scheme may not provide the services on behalf of the government directly. Instead, the NPOs may serve as "sponsors" to third-party fraudulent entities that purport to provide government services. In return for acting as a sponsor, an NPO may be entitled to certain administrative fees from the government.[44] In connection with such schemes, the NPO sponsor may not only receive government reimbursement but may also receive kickbacks from the fraudulent third party that purports to provide the services.[45]

Case Study: Charity Executive Director Agrees to Plead Guilty to Homelessness Funds Fraud[46]

In California, the City of Los Angeles, Los Angeles County, and other public entities provide funding for homeless housing and services through programs administered by the Los Angeles Homeless Services Authority (LAHSA). LAHSA, in turn, disburses funds to third-party entities to provide services to the homeless. In one case, a defendant agreed to plead guilty to participating in a scheme in which the NPO he founded contracted with LAHSA to provide homelessness services but failed to provide the required services. According to court documents, the defendant lied to LAHSA about how he was using the taxpayer money his charity received, falsely stating that he used it exclusively to combat the homelessness crisis in Los Angeles, when he was misappropriating millions of dollars for himself. Among other things, the defendant moved funds from the NPO's account to accounts controlled by him.

43. *See* FinCEN, FIN-2026-Alert001, "FinCEN Alert on Fraud Rings and Their Exploitation of Federal Child Nutrition Programs in Minnesota" (Jan. 9, 2026); *see, e.g.*, DOJ, U.S. Attorney's Office for the Western District of Michigan, Press Release, "Former CEO of West Michigan Nonprofit Sentenced to 70 Months in Federal Prison" (May 13, 2026).
44. *See, e.g.*, DOJ, Press Release, "Feeding Our Future Ringleader Sentenced to 500 Months" (May 22, 2026) [hereinafter "Minnesota Fraud Press Release"].
45. *See, e.g., id*.
46. *See* DOJ, Press Release, "Two Defendants Employed at L.A.-Area Homeless Nonprofits Arrested on Federal Charges Alleging Misuse of Millions of Taxpayer Dollars" (Sept. 16, 2026); Plea Agreement for Defendant Alexander Soofer, *United States v. Soofer*, No. 2:26-cr-00077-MWF (C.D. Cal. Sept. 16, 2026), ECF No. 63 [hereinafter "LAHSA Fraud Plea Agreement"].

The defendant lied about payments supposedly being made to third-party vendors for homeless housing services and took steps to conceal that he was diverting the money to his personal bank accounts. Among other actions, the defendant lied about rent payments being made for properties he was supposed to be using for housing for homeless individuals and families, making it falsely appear that he was leasing these properties from third-party landlords at a market rate, when he was instead paying himself above-market-rate rent. Additionally, the defendant provided substandard meals to the homeless (in violation of the contract with LAHSA).

NPO Fraud Typologies and Misappropriation Techniques

Bad actors use various methods to access and use NPO funds in NPO fraud schemes. In certain cases, managers may directly use NPO funds to purchase goods or services (such as real estate, vehicles, travel and entertainment, and luxury goods), make investments (including investments related to digital assets), or gamble for personal gain. To engage in these transactions, they may use NPO accounts or credit cards, or they may transfer money to personal accounts or accounts held by relatives or friends.[47] In other instances, NPO managers may misappropriate NPO funds by having ostensible third-party firms that are actually under their control contract with the NPO. These third-party entities may engage in phantom billing, the practice of invoicing the NPO for a good or service that was never provided, to channel money from the NPO's accounts to their own.[48] Alternatively, NPO managers may use firms under their control to provide goods or services that are exploitative, substandard, or unnecessary and keep the difference in cost between the goods and services contracted for and the goods and services actually provided.[49] NPO management may use transactions involving cash or digital assets in an effort to conceal its misappropriation of funds. In certain cases, NPO management may also misappropriate funding by using restricted funds for unapproved purposes, such as political activity.[50]

The percentage of misappropriated funds may vary among schemes. In certain cases, the NPO may deliver few or no services, misappropriating all or most of the NPO's funds.[51] In other cases, the NPO may provide services but also use a portion of the funds for illicit purposes.[52] The degree of misappropriation may also vary over time. For example, an NPO may increase the scope of its

47. *See, e.g.*, DOJ, U.S. Attorney's Office for the Southern District of New York, Press Release, "Founder and Former CEO of Charity Pleads Guilty to Multimillion-Dollar Charity Fraud and Tax Evasion" (Aug. 18, 2025) [hereinafter "Modest Needs Fraud Press Release"]; DOJ, U.S. Attorney's Office for the District of Minnesota, Press Release, "Big Lake Woman Pleads Guilty to Wire Fraud in $250 Million Feeding Our Future Fraud Scheme" (Jan. 10, 2024).
48. *See, e.g.*, IRS, "Former Executive of Chicago-Area Non-Profit Sentenced to Prison for $1.9 Million Fraud Schemes" (Apr. 8, 2026).
49. *See, e.g.*, LAHSA Fraud Plea Agreement, *supra* note 46.
50. *See, e.g.*, DOJ, U.S. Attorney's Office for the Western District of Missouri, Press Release, "Former Charity CEO Pleads Guilty to Multi-Million-Dollar Political Corruption Scheme" (Nov. 13, 2018).
51. *See, e.g.*, Massachusetts Office of the Attorney General, Press Release, "AG Campbell Secures Court Orders Permanently Barring Operators of a Fraudulent Veterans Charity from Engaging in Charitable Activities in Massachusetts" (Mar. 30, 2026).
52. *See, e.g.*, Modest Needs Fraud Press Release, *supra* note 47; Minnesota Fraud Press Release, *supra* note 44.

misappropriation of funds to take advantage of different funding opportunities or a sudden influx of funds, such as from relief programs established during the COVID-19 pandemic.[53]

In other NPO fraud schemes, fraudsters will take advantage of the benefits provided by NPOs rather than using the NPO as a means of defrauding donors. For example, by funneling transactions through an NPO they control, they may evade taxes or avoid the payment of other fees.[54]

NPO Embezzlement Schemes

In NPO embezzlement schemes, NPO insiders embezzle money from an NPO that is operating for legitimate purposes. In these cases, the majority of both the NPO's employees and its donors are typically unaware of the embezzlement, and the NPO itself is a victim of the scheme.

The insiders perpetrating NPO embezzlement schemes may be members of the NPO's management abusing their positions of trust and authority, even while the rest of the NPO's staff is unaware of the embezzlement.[55] Alternatively, the insiders may simply be individuals with access to NPO funds.[56] The perpetrators could also be third-party contractors with access to the NPO's finances.[57]

Generally, the insiders may use many of the same methods noted above to misappropriate NPO funds. They may directly use NPO accounts for personal expenses or transfer funds from NPO accounts into personal accounts to purchase goods or services (such as real estate, vehicles, travel and entertainment, and luxury goods), make investments (including investments related to digital assets), or gamble for personal gain. Insiders may also divert donations meant for the NPO, preventing the NPO from receiving the funds. For example, in one case, an insider deposited a check intended for the NPO into his personal account.[58]

Like bad actors in NPO fraud schemes, embezzlers may take advantage of their role as insiders to contract with ostensible third-party entities that are actually under embezzlers' control, entities which they then use to invoice the defrauded NPO while providing no services.[59] Alternatively,

53. *See, e.g.*, DOJ, U.S. Attorney's Office for the Eastern District of Missouri, Press Release, "Nonprofit Exec Sentenced to 16 Years in Prison for the Largest Public Assistance Fraud in Missouri History" (Mar. 16, 2026).
54. *See, e.g.*, DOJ, Press Release, "Colorado Man Pleads Guilty to Years-Long Scheme to Defraud the IRS and for Operating a Multi-Million Dollar Investment Fraud Scheme" (Aug. 8, 2025); DOJ, U.S. Attorney's Office for the Western District of Missouri, Press Release, "Former NBA Player Sentenced for False Tax Returns, Identity Theft Related to Charity Fraud Scheme" (July 9, 2018).
55. *See, e.g.*, DOJ, U.S. Attorney's Office for the Eastern District of New York, Press Release, "Former Executive Director and Former Employee of Queens Defenders Legal Services Non-Profit Sentenced to Prison for Embezzling Funds" (July 28, 2026).
56. *See, e.g.*, DOJ, U.S. Attorney's Office for the Eastern District of Missouri, Press Release, "Former Charity Employee Sentenced to 40 Months in Prison for Stealing Nearly $700,000" (Sept. 18, 2025).
57. *See, e.g.*, DOJ, U.S. Attorney's Office for the Eastern District of Virginia, Press Release, "Administrator of Charity Program for Virginia State Employees Sentenced for Stealing Over $1.5M" (May 13, 2026) [hereinafter "Virginia Charity Fraud Press Release"].
58. *See, e.g.*, DOJ, U.S. Attorney's Office for the Northern District of California, Press Release, "Former Executive Director Who Embezzled Over $500,000 from Non-Profit Serving Oakland Youth Sentenced to More Than Two Years in Prison" (Sept. 24, 2025).
59. *See, e.g.*, DOJ, U.S. Attorney's Office for the Eastern District of New York, Press Release, "Former Fiscal Officer for Non-Profit Company Pleads Guilty to Stealing Nearly $2.3 Million from Brooklyn Charity" (Jan. 19, 2024).

they may contract with third-party vendors and receive kickbacks.[60] Bad actors may attempt to conceal their embezzlement by withdrawing funds in cash or using digital assets.[61] In some cases, NPO embezzlement schemes may overlap with NPO fraud schemes. For example, an employee of a legitimate NPO may—without the NPO management's knowledge—obtain funding from a government source through fraudulent means and then embezzle a portion of those funds.[62]

However, unlike in NPO fraud schemes, bad actors in NPO embezzlement schemes conceal their misappropriation not just from donors but also from non-complicit NPO management and employees. For example, embezzlers may use or create accounts that are not visible to other NPO employees or officers or file additional fraudulent paperwork to justify expenses with complicit third-party entities. To cover their tracks, insiders may also deposit money from personal accounts or other sources back into the defrauded NPO's accounts.[63]

Case Study: Administrator of Charity Program for Virginia State Employees Sentenced for Stealing Over $1.5 Million[64]

In 2026, a woman was sentenced to four years in prison for stealing more than $1.5 million from the Commonwealth of Virginia Campaign (the "Campaign"), the officially sanctioned non-profit charity fundraising program for Virginia's more than 120,000 state government employees. According to court documents, from 2017 through 2023, the Virginia Department of Human Resources Management employed the defendant as a contractor to administer the Campaign. As the steward of these funds, the contractor was responsible for making corresponding payments to charities designated by donors. Between January 2019 and August 2023, the contractor embezzled more than $1.5 million of the over $5.3 million donated by state government employees. The defendant pleaded guilty to misappropriating the money by transferring funds from an NPO account she controlled to her personal account and directing donor money to personal accounts as opposed to the official account for the NPO.

60. *See, e.g.*, DOJ, U.S. Attorney's Office for the Western District of Pennsylvania, Press Release, "Former Primary Health Network CEOs Sentenced to Prison for Defrauding Non-Profit Medical Organization of Millions of Dollars" (Apr. 24, 2026).
61. *See, e.g.*, DOJ, U.S. Attorney's Office for the Central District of Illinois, Press Release, "Former Treasurer of Illinois State Police Heritage Foundation Pleads Guilty to Defrauding Foundation" (Mar. 8, 2024).
62. *See, e.g.*, Manhattan District Attorney's Office, Press Release, "Manhattan D.A. Bragg, Comptroller DiNapoli Announce Guilty Plea of Former NYU Director of Finance for Major Fraud" (Feb. 26, 2024).
63. *See, e.g.*, DOJ, U.S. Attorney's Office for the Southern District of Indiana, Press Release, "Former Indiana University Foundation Employee Sentenced to One Year in Federal Prison for Embezzling More Than $326,000 in Donations" (Nov. 8, 2023); DOJ, U.S. Attorney's Office for the Eastern District of Michigan, Press Release, "Former Detroit Riverfront Conservancy CFO Pleads Guilty to Embezzling Over $40 million from Conservancy" (Nov. 15, 2024).
64. *See* Virginia Charity Fraud Press Release, *supra* note 57; Statement of Facts, *United States v. Brown*, No. 3:25-cr-00141-RCY (E.D. Va. Oct. 7, 2025), ECF No. 16.

Red Flag Indicators of NPO Abuse

FinCEN has identified the following red flags to help financial institutions detect, prevent, and report suspicious activity connected to schemes involving NPOs. 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 whether a behavior or transaction is suspicious.

FinCEN reminds financial institutions that no customer type presents a single level of uniform risk or a particular risk profile related to money laundering, terrorist financing, or other illicit financial activity.[65] As part of the risk-based approach, financial institutions should ensure that their preventive and mitigation measures are commensurate with their relevant risks in order to avoid unintended consequences that unduly disrupt or discourage legitimate NPO activities. Furthermore, financial institutions are reminded that it is the policy of the United States that no American should be denied access to financial services because of their constitutionally or statutorily protected beliefs, affiliations, or political views and that politicized or unlawful debanking is not used as a tool to inhibit such beliefs, affiliations, or political views.[66]

Although the BSA does not require the collection of specific NPO-related information, certain customer information may be useful for financial institutions in determining the risk profile of NPO customers. Financial institutions may consider collecting general information about an NPO's donor base, funding sources, and fundraising methods (including foreign funding for U.S.-based NPOs), and an NPO's affiliation with other NPOs, governments, or groups.[67]

Red flags related to an NPO and its officers or employees:

1. A customer that is an NPO solicits donations but does not appear to provide any services, has limited operations, or has little or no physical or online presence. For example, the address for the NPO may be a post office box, an address that does not appear to correspond to an NPO (such as a residential address or unrelated business), or an address shared by many different NPOs. Alternatively, the NPO may have no employees or no website or a dated or generic website.

2. A customer that is an NPO has a name similar to an existing or well-known NPO but does not appear to have any affiliation with it.

3. A customer that is an NPO openly supports terrorist or criminal activity or operations (such as in fundraising appeals or on social media) or includes, in the information related to a transaction between customers or the notes accompanying peer-to-peer transfers, key terms known to be associated with terrorism or terrorist organizations.

65. *See* Federal Reserve, FDIC, FinCEN, NCUA, OCC, "Joint Statement on the Risk-Based Approach to Assessing Customer Relationships and Conducting Customer Due Diligence" (July 6, 2022).
66. *See* Fair Banking E.O., *supra* note 4.
67. NPO Fact Sheet, *supra* note 3, at 3.

4. A customer that is an NPO is not registered with the appropriate state regulator (to the extent required in the relevant state) or cannot verify its legal operating status to the financial institution.

5. An individual with previous fraud convictions is a signatory to an NPO account or is an officer, employee, or contractor of an NPO.

6. A customer that is an NPO has been in existence for many years and, for no apparent lawful or business purpose, opens a new account, which may have signatories that differ from—or only partially overlap with—the signatories on its existing NPO accounts.

Red flags related to sources of funds:

7. A customer that is an NPO receives funds for multiple causes that appear unrelated to each other or from multiple unrelated crowdfunding platforms or campaigns or receives funds with notes indicating support for unrelated causes.

8. A customer that is an NPO receives large donations from an unknown source over a short period of time and then sends significant wire transfers or checks to other NPOs.

9. A customer that is a recently established NPO suddenly receives a significant number of donations or reimbursements in a short timeframe, including in connection with a disaster or other emergency, inconsistent with the customer profile of other similar entities.

10. A customer that is a recently established NPO starts receiving an unusually high volume of payments, payments in unusually large amounts, or reimbursements from government aid programs soon after starting its operations.

11. A customer that is an NPO receives unexplained funds from personal accounts of officers, employees, or contractors of the NPO, or other sources of funds that do not appear to be consistent with donations.

12. A customer that is an NPO employee, officer, or contractor receives, in an account used for personal expenditures, payments or credits that are addressed to or intended for the NPO itself rather than the employee, officer, or contractor.

13. Multiple customers that are NPOs have the same or similar signatories or controllers, but they receive funding from different government sources for unrelated services.

14. A customer that is not an NPO receives incoming payments or credits that reference NPO activity, such as charitable giving, fundraising campaigns, or humanitarian causes.

Red flags related to uses of funds:

15 A customer that is an NPO, or the employee, officer, or contractor of an NPO, exhibits spending patterns that are not commensurate with the customer's known financial profile or that of similarly situated NPOs or NPO officials, including expenditures indicative of unexplained wealth or sudden changes in wealth. For example, the customer engages in significant transactions with broker-dealers, commodities and futures exchanges, money services businesses (including those involved in digital assets), or casinos or gambling establishments or has significant transactions related to personal expenses or retail point-of-sale transactions.

16 A customer that is an NPO has minimal or no operating costs other than purchases of ads on social media.

17 A customer that is an NPO has minimal or no operating costs other than payments for "consulting fees" or for other vague or repetitive invoices (e.g., "food supplies").

18 A customer that is an NPO, or the employee, officer, or contractor of an 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) or avoid recordkeeping requirements.[68]

19 A customer that is an NPO, or the employee, officer, or contractor of an NPO, makes a significant amount of cash withdrawals or deposits or frequently purchases or redeems cashier's checks for no clear purpose.

20 A customer that is an NPO focused on providing services in the United States sends a significant amount of funds to individuals and companies located in foreign jurisdictions.

21 A customer that is an NPO makes unexplained or one-off payments to managers, employees, contractors, or board members that are inconsistent with expected payroll patterns.

22 A customer that is an NPO conducts transactions with accounts that have the same signatories as the NPO's accounts or transactions with family members, friends, or associates of NPO employees, officers, or contractors.

68. *See* generally 31 C.F.R. §§ 1010.100(xx), 1010.314, 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 omitted)).

Reminder of Relevant BSA Obligations and Tools for U.S. Financial Institutions

Suspicious Activity Reporting

A financial institution is required to file a suspicious activity report (SAR) if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity; is intended or conducted to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity.[69] All statutorily defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.[70]

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR.[71] Financial institutions must provide any requested documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency.[72] When requested to provide supporting documentation, financial institutions should take special care to verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. A financial institution should incorporate procedures for such verification into its BSA compliance or AML program. These procedures may include, for example, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.

SAR Filing Instructions

SARs, and compliance with other BSA requirements, are crucial to identifying and stopping abuse of NPOs. FinCEN requests that financial institutions indicate a connection between the suspicious activity being reported and the activities highlighted in this Notice by including the key term "**FIN2026NPO**" in SAR field 2 (Filing Institution Note to FinCEN), as well as in the narrative. Financial institutions may highlight additional Advisory, Alert, or Notice keywords in the narrative, if applicable.

Financial institutions should include all available information relating to the account and locations involved in the reported activity, identifying information related to other entities and persons involved in the activity and the status of their accounts with the institution. Financial institutions also should provide all available information regarding other domestic and foreign financial institutions involved in the activity; where appropriate, financial institutions should consider filing a SAR jointly on shared suspicious activity.[73]

69. *See* 31 U.S.C. § 5318(g)(1); *see also* 31 C.F.R. §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, 1030.320.
70. *See* 31 U.S.C. § 5318(g)(3). Financial institutions may report suspicious transactions regardless of amount involved and still take advantage of the safe harbor.
71. *See* 31 C.F.R. §§ 1020.320(d), 1021.320(d), 1022.320(c), 1023.320(d), 1024.320(c), 1025.320(d), 1026.320(d), 1029.320(c), 1030.320(c).
72. *See id.*; *see also* FinCEN, FIN-2007-G003, "Suspicious Activity Report Supporting Documentation" (June 13, 2007).
73. *See* 31 C.F.R. §§ 1020.320(e)(1)(ii)(A)(2)(i), 1021.320(e)(1)(ii)(A)(2), 1022.320(d)(1)(ii)(A)(2), 1023.320(e)(1)(ii)(A)(2)(i), 1024.320(d)(1)(ii)(A)(2), 1025.320(e)(1)(ii)(A)(2), 1026.320(e)(1)(ii)(A)(2)(i), 1029.320(d)(1)(ii)(A)(2), 1030.320(d)(1)(ii)(A)(2).

Financial institutions are required to file complete and accurate reports that incorporate all relevant information available. Any financial institution and any director, officer, employee, or agent of such institution who makes, or requires another to make any voluntary disclosure of any possible violation of law or regulation to a government agency under the BSA or its implementing regulations is protected from liability for any such disclosure.[74]

In situations involving violations requiring immediate attention, such as ongoing money laundering schemes, a financial institution should also immediately notify, by telephone, an appropriate law enforcement authority, in addition to filing a timely SAR.[75] Immediate notification to law enforcement is especially important in situations involving suspected terrorist activity, as terrorists and terrorist organizations often rely on the international financial system to acquire funding to sustain and finance their operations and engage in acts of terrorism.

Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).[76]

Other Relevant BSA Reporting Requirements

Financial institutions and other entities or persons may also have other relevant BSA reporting requirements to provide information in connection with the subject of this Notice. These include obligations related to the Currency Transaction Report (CTR),[77] Report of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300),[78] Report of Foreign Bank and Financial Accounts (FBAR),[79] Report of International Transportation of Currency or Monetary Instruments (CMIR),[80] Registration of Money Services Business (RMSB),[81] and Designation of Exempt Person (DOEP).[82]

74. 31 U.S.C. § 5318(g)(3); *see, e.g.*, 31 C.F.R. § 1020.320(f).
75. *See, e.g.*, 31 C.F.R. §§ 1020.320(b)(3), 1022.320(b)(3), 1023.320(b)(3).
76. The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.
77. A report of each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through, or to a financial institution that involves a transaction in currency of more than $10,000. Multiple transactions may be aggregated when determining whether the reporting threshold has been met. *See* 31 C.F.R. §§ 1010.310-313, 1020.310-313, 1021.310-313, 1022.310-313, 1023.310-313, 1024.310-313, and 1026.310-313.
78. A report filed by a trade or business that receives currency in excess of $10,000 in one transaction or two or more related transactions. The transactions are required to be reported on a joint FinCEN/Internal Revenue Service form when not otherwise required to be reported on a CTR. *See* 31 C.F.R. § 1010.330. A Form 8300 also may be filed voluntarily for any suspicious transaction, even if the total amount does not exceed $10,000.
79. A report filed by a U.S. person that has a financial interest in, or signature or other authority over, foreign financial accounts with an aggregate value exceeding $10,000 at any time during the calendar year. *See* 31 C.F.R. § 1010.350; FinCEN Form 114.
80. A form filed to report the transportation of more than $10,000 in currency or other monetary instruments into or out of the United States. *See* 31 C.F.R. § 1010.340.
81. A form filed to register a money services business (MSB) with FinCEN, or to renew such a registration. *See* 31 C.F.R. § 1022.380.
82. A report filed by banks to exempt certain customers from currency transaction reporting requirements. *See* 31 C.F.R. § 1020.315.

Form 8300 Filing Instructions

When filing a Form 8300 involving a suspicious transaction relevant to this Notice, FinCEN requests that the filer select ***Box 1b*** ("suspicious transaction") and include the key term "**FIN2026NPO**" in the "Comments" section of the report.

Due Diligence

Banks, brokers or dealers in securities, mutual funds, and futures commission merchants and introducing brokers in commodities are required to have appropriate risk-based procedures for conducting ongoing customer due diligence that include, but are not limited to: (i) understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and (ii) conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.[83] Covered financial institutions are required to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions.[84] Among other things, this facilitates the identification of legal entities that may be owned or controlled by foreign politically exposed persons.

Senior foreign political figures and due diligence obligations for private banking accounts

In addition to these due diligence obligations, under section 312 of the USA PATRIOT Act (31 U.S.C. § 5318(i)) and its implementing regulations, covered financial institutions must implement due diligence programs for private banking accounts held for non-U.S. persons that are designed to detect and report any known or suspected money laundering or suspicious activity conducted through or involving such accounts.[85] Covered financial institutions must establish risk-based controls and procedures for ascertaining the identities of nominal and beneficial owners of such accounts and ascertaining whether any of these owners are senior foreign political figures, and for conducting enhanced scrutiny on accounts held by senior foreign political figures that is reasonably designed to detect and report transactions that may involve the proceeds of foreign corruption.[86]

AML/CFT program and correspondent account due diligence requirements

Financial institutions are reminded of AML/CFT program requirements,[87] and covered financial institutions are reminded of correspondent account due diligence requirements under Section 312 of the USA PATRIOT Act (31 U.S.C. § 5318(i)) and implementing regulations.[88] As described in

83. *See* 31 C.F.R. §§ 1020.210(a)(2)(v), 1023.210(b)(5), 1024.210(b)(6), 1026.210(b)(5).
84. *See* 31 C.F.R. §§ 1010.230(f), 1010.605(e)(1) (defining "covered financial institution").
85. *See* 31 C.F.R. § 1010.620. The definition of "covered financial institution" is found in 31 C.F.R. § 1010.605(e)(1). The definition of "private banking account" is found in 31 C.F.R. § 1010.605(m). The definition of "non-U.S. person" is found in 31 C.F.R. § 1010.605(h).
86. *See* 31 C.F.R. § 1010.620(c).
87. *See* 31 C.F.R. §§ 1010.210, 1020.210, 1021.210, 1022.210, 1023.210, 1024.210, 1025.210, 1026.210, 1027.210, 1028.210, 1029.210, 1030.210.
88. *See* 31 C.F.R. § 1010.610.

FinCEN Interpretive Release 2004-1, the AML/CFT program of an MSB must include risk-based policies, procedures, and controls designed to identify and minimize risks associated with foreign agents and counterparties.[89]

Information Sharing

Information sharing between and among financial institutions is critical to identifying, reporting, and preventing illicit activity, including abuse of NPOs. Under the safe harbor from liability provided by section 314(b) of the USA PATRIOT Act, financial institutions may share information with other eligible financial institutions regarding activities that may involve possible terrorist activity or money laundering, including information about fraud and other specified unlawful activities.[90] FinCEN strongly encourages financial institutions to participate in this voluntary program as information sharing between and among financial institutions can assist financial institutions in managing illicit financing risks and can ultimately provide the government with highly useful information to identify and prevent financial crime. Given the transnational nature of illicit activity, FinCEN encourages U.S. financial institutions to use, and potentially expand, their processes to collect and share information with foreign financial institutions to further investigations involving cross-border activity.[91]

The section 314(b) program provides financial institutions with the flexibility and connectivity needed to counter threats and prevent illicit actors from exploiting gaps between institutions. Among other things, information sharing pursuant to section 314(b) allows financial institutions to respond to threats—activities a financial institution suspects may involve possible terrorist activity or money laundering, such as fraud and other criminal activity—that are carried out by repeat actors moving across financial institutions to evade detection.

For additional information, see FinCEN's Section 314(b) Fact Sheet.

89. *See* FinCEN, Interpretive Release 2004-1, "Anti-Money Laundering Program Requirements for Money Services Businesses with Respect to Foreign Agents or Foreign Counterparties," 69 Fed. Reg. 74,439 (Dec. 14, 2004); *see also* FinCEN, FIN-2016-G001, "Guidance on Existing AML Program Rule Compliance Obligations for MSB Principals with Respect to Agent Monitoring" (Mar. 11, 2016).
90. *See* 31 C.F.R. § 1010.540; *see also* FinCEN, "Section 314(b) Fact Sheet" (June 12, 2026).
91. *See* FinCEN, FIN-2025-G001, "Cross-Border Information Sharing by Financial Institutions and SAR Confidentiality" (Sept. 5, 2025).

FinCEN's Whistleblower Program

FinCEN maintains a whistleblower incentive program for violations of the BSA and certain national security laws such as the International Emergency Economic Powers Act. Individuals located in the United States or abroad who provide information may be eligible for awards if the information they provide leads to a successful enforcement action that results in monetary penalties exceeding $1,000,000 and the statutory requirements in 31 U.S.C. § 5323 are otherwise met. Under 31 U.S.C. § 5323, there are certain confidentiality protections for individuals submitting information as well as certain protections from retaliation by employers. Individuals may also choose to submit information anonymously to FinCEN, including through an attorney. FinCEN is currently accepting whistleblower tips and encourages those with knowledge of potential violations to contact FinCEN. To learn more about FinCEN's Whistleblower Program, visit https://www.fincen.gov/whistleblower-program.

FinCEN's Advisory Program communicates priority money laundering, terrorist financing, and other illicit finance threats and vulnerabilities to the U.S. financial system. Financial institutions may use this information to support effective, risk-based, and reasonably designed AML/CFT programs and suspicious activity monitoring systems to help generate highly useful information for law enforcement and national security agencies.

For Further Information

FinCEN's website at www.fincen.gov contains information on how to register for FinCEN Updates. Questions or comments regarding the contents of this Notice should be addressed to the FinCEN Regulatory Support Section by submitting an inquiry at ois.fincen.gov/contact/.

FinCEN's mission is to safeguard the financial system from illicit activity, 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.