



Statement of

Rena S. Miller

Specialist in Financial Economics

Before

Committee on Financial Services

Subcommittee on National Security, International Development, and
Monetary Policy

U.S. House of Representatives

Hearing on

**“A Persistent and Evolving Threat: An
Examination of the Financing of Domestic
Terrorism and Extremism”**

January 15, 2020

Congressional Research Service

7-5700

www.crs.gov

Chairman Cleaver, Ranking Member Hill, Members of the Subcommittee, thank you for the opportunity to testify today. My name is Rena Miller, and I have been a Specialist in Financial Economics at the Congressional Research Service (CRS) since 2009, focusing on financial regulation including anti-money laundering and terrorism financing issues. My testimony will first discuss the current regulatory tools upon which the nation’s counter terrorism financing system relies.¹ It will then examine the ways in which those existing tools may face challenges because of the evolving methods for financing domestic terrorism and home-grown violent extremism (HVE). For brevity, I will use the term “domestic terrorism” to include HVEs and other domestic actors, but I will also examine U.S. actors providing support to foreign terrorist organizations as relevant. Lastly, I will touch upon changing technologies and legislative proposals such as beneficial ownership legislation (H.R. 2513) and financial intelligence legislation (H.R. 5132). I would note that CRS is nonpartisan and does not advocate for any policies or proposals.

Basis of U.S. Regime to Counter Terrorism Financing

The existing U.S. regulatory regime to combat terrorism financing was not set up specifically with the challenges of small-scale domestic terrorism in mind. The existing regime draws heavily upon both the Bank Secrecy Act of 1970,² known as the BSA, and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001,³ known as the USA PATRIOT Act, passed in the wake of the Sept. 11, 2001 terrorist attacks.

The United States enacted anti-money laundering (AML) legislation partly in response to money laundering from the illicit drug trade, to make it harder for large amounts of cash or unexplained money deposited to be made to look “clean.” The BSA required financial institutions to file certain reports to the Treasury Department’s Financial Crimes Enforcement Network (FinCEN) and maintain records for their account holders.⁴ Prominent among these reports are “suspicious activity reports,” known as SARs, and “currency transaction reports,” or CTRs. CTRs must be filed automatically by banks when a customer withdraws or deposits \$10,000 or more in cash.

This filing requirement was later expanded to retailers receiving \$10,000 or more in cash. But these requirements are specific to *cash* transactions—so the form of the payment matters. The IRS considers cash to include traveler’s checks, cashier checks, bank drafts and money orders, but electronic payments such as credit cards and cryptocurrencies are not included.⁵ CTRs have historically been most useful for identifying money laundering by criminals involved in cash-intensive illicit activities. In an increasingly cashless society, they may be less relevant in flagging potential domestic terror attacks—particularly for small-scale attacks that may not require large sums, such as those involving retail firearms or a rented car.

SARs may prove useful in flagging suspicious money transfers, for example between U.S. account holders and “high risk” terrorism jurisdictions. But if such overseas payments are not used frequently in

¹ For further information, see CRS Report R44776, *Anti-Money Laundering: An Overview for Congress*, by Rena S. Miller and Liana W. Rosen; CRS In Focus IF11061, *Targeting Illicit Finance: The Financial Crimes Enforcement Network’s “Financial Institution Advisory Program”*, by Liana W. Rosen and Rena S. Miller; CRS In Focus IF10873, *Overview of Correspondent Banking and “De-Risking” Issues*, by Rena S. Miller.

² The Bank Secrecy Act of 1970, 12 U.S.C. §§1829b and 1951-1959, and 31 U.S.C. 5311-5322, and its major component, the Currency and Foreign Transactions Reporting Act, 31 U.S.C. §§5311-5322.

³ The International Money Laundering Abatement and Anti-Terrorist Financing Act, Title III of the USA-PATRIOT Act, P.L. 107-56.

⁴ Tracey Durner and Danielle Cotter, “Untangling a Marriage of Convenience: Anti-Money Laundering and Countering the Financing of Terrorism,” Global Center on Cooperative Security, January 2019.

⁵ See <https://www.irs.gov/businesses/small-businesses-self-employed/irs-form-8300-reference-guide> and <https://www.californiacannabiscpa.com/blog/irs-audits-and-form-8300-what-is-it-and-why-is-it-important>.

small-scale domestic attacks, the usefulness of SARs in this realm to prevent attacks may be more attenuated. CTRs, SARs and other BSA reports can often provide valuable information to law enforcement following such attacks,⁶ even if their usefulness to flag potential attacks may be more circumspect. Following an actual attack, publicized event, or in response to other “derogatory information” available to them, financial institutions may proactively file SARs or provide other information to FinCEN which can then prove useful to law enforcement in their investigation. A 2018 assessment by the Treasury Department of SAR filings associated with U.S.-based individuals charged with supporting terrorist activity found that most were filed based on derogatory information regarding the sender or recipient, rather than based on suspicious activity associated with the transaction itself.⁷ When there is more information in the public realm about domestic terrorist actors and their financing, financial institutions may be more likely to proactively provide such information.

The USA PATRIOT Act also introduced additional customer due diligence (CDD) procedures for financial institutions opening accounts.⁸ This CDD rule was amended by FinCEN, effective in 2018, to include some due diligence associated with the identities of beneficial owners, who may control or benefit from an entity but not be its registered owner.⁹ While these measures assist law enforcement in cracking down on money laundering and other illicit use of the financial system, they rely on customers’ use of accounts at banks and brokerage firms. If domestic terrorists don’t rely on such accounts, or on international wire transfers and overseas remittances into or out of such accounts, then a reporting regime and customer due diligence requirements may prove less effective for flagging would-be domestic terrorists. Even for terrorism with an international nexus, the 2018 Treasury assessment found that, “An additional challenge for financial institutions is that many transactions associated with terrorism financing are often hard to distinguish from legitimate day-to-day transactional activity.”¹⁰

Another pillar of the nation’s post-9/11 Countering Financing of Terrorism (CFT) regime has been the designation of foreign terrorist organizations (FTOs) and the freezing of their assets, as well as “secondary sanctions” wherein correspondent banks “freeze out” designated groups or individuals from dollar-denominated transfers into or out of the U.S. financial system.¹¹ Broadly, these authorities stem from Executive Order 13224, first signed by President George W. Bush after 9/11 in 2001, and issued under the International Emergency Economic Powers Act (IEEPA).¹² These measures can have potent effects on state actors or large, established entities—especially if those actors rely on transactions with the United States and can’t easily continue operations under an assumed identity. Yet domestic terrorism may involve previously unknown individuals.

⁶ See, e.g., “We are already able to confirm just how extensive and crucial the value of BSA reporting is to an array of stakeholders and activities—activities that go well beyond just whether or not a particular SAR, CTR, or FBAR (or any other BSA report) facilitates a particular law enforcement investigation.” Kenneth A. Blanco, Director, *Prepared Remarks of FinCEN Director Blanco at the NYU Law Program on Corporate Compliance and Enforcement*, Financial Crime Enforcement Network, June 12, 2019, <https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-blanco-nyu-law-program-corporate-compliance-and>.

⁷ Department of Treasury, *National Terrorism Financing Risk Assessment*, 2018, p. 20.

⁸ 31 U.S.C. §5318(l). See Joint Final Rule—Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks.

⁹ Financial Crimes Enforcement Network (FinCEN), Treasury, “Customer Due Diligence Requirements for Financial Institutions,” 81 *Federal Register* 29398, May 11, 2016.

¹⁰ Department of Treasury, *National Terrorism Financing Risk Assessment*, 2018, Executive Summary.

¹¹ For more information, see CRS Report R41333, *Terrorist Material Support: An Overview of 18 U.S.C. §2339A and §2339B*, by Charles Doyle.

¹² Peter R. Neumann, “Don’t Follow the Money: The Problem with the War on Terrorist Financing,” 96 *Foreign Aff.* 93 (2017).

Also, such public designations—of particular relevance for the financial sector in screening customers—only apply to foreign terrorist organizations, not domestic groups.¹³ This may reflect First Amendment concerns.¹⁴ The current designations have at times resulted in significant sums of money frozen for foreign state sponsors of terrorism and FTOs. By contrast, domestic extremists appear to be less well-funded, may rely on newer online methods of fund-raising, and may require relatively limited funds for their attacks. They may be harder for banks to screen—assuming they use banks at all—particularly if they have no prior convictions or other red flags. Though the United States may have potent regulatory tools to combat financing terrorism of larger FTOs and state sponsors, these tools may be harder to leverage in the realm of domestic terrorism.

The New Challenges of Domestic Terrorism Financing

I will briefly discuss domestic terrorism itself; then what we know about its financing; and finally, the new challenges this poses for the existing AML/CFT regime.

Threat of Domestic Terrorism

In the United States, domestic terrorism is defined by statute as a life-endangering federal or state crime, committed within the United States, with the apparent intent to coerce or intimidate a civilian population or influence government policy or conduct.¹⁵ Federal Bureau of Investigation (FBI) Director Christopher Wray, in November 2019, called home-grown violent extremists (HVEs) “the greatest, most immediate terrorism threat to the homeland.”¹⁶ He noted that these individuals are inspired by foreign terrorist organizations, but have been radicalized primarily in the United States, and are not receiving individualized direction from overseas groups.¹⁷ Previous testimony by a senior FBI official noted:

domestic terrorists pose a present and persistent threat of violence and economic harm to the United States; in fact, there have been more arrests and deaths caused by domestic terrorists than international terrorists in recent years. We are most concerned about lone offenders, primarily using firearms, as these lone offenders represent the dominant trend for lethal domestic terrorists. Frequently, these individuals act without a clear group affiliation or guidance, making them challenging to identify, investigate, and disrupt.¹⁸

According to the FBI, the possible underlying drivers for domestic terrorism include perceptions of government or law enforcement overreach, socio-political conditions, racism, anti-Semitism,

¹³ The government does not provide an official and public list of domestic terrorist organizations, but includes known and suspected domestic terrorists (along with international terrorists) in its Terrorist Screening Database, commonly known as the “Terrorist Watchlist.” This contrasts to the world of international counterterrorism, where the United States maintains a well-established regimen regarding the identification of foreign terrorist organizations. See CRS Report R44921, *Domestic Terrorism: An Overview*, by Jerome P. Bjelopera, Specialist in Organized Crime and Terrorism, August 21, 2017, p. 57.

¹⁴ See CRS Report R44921, *Domestic Terrorism: An Overview*, by Lisa N. Sacco; and CRS Legal Sidebar LSB10340 *Domestic Terrorism: Some Considerations*, by Charles Doyle, August 12, 2019.

¹⁵ 18 U.S.C. §2331. For further detail, please see CRS Legal Sidebar LSB10340 *Domestic Terrorism: Some Considerations*, by Charles Doyle, August 12, 2019.

¹⁶ Christopher Wray, Director, Federal Bureau of Investigation, *Worldwide Threats*, Statement Before the Senate Homeland Security and Governmental Affairs Committee, Washington, D.C., November 5, 2019, <https://www.fbi.gov/news/testimony/worldwide-threats-110519>.

¹⁷ Ibid.

¹⁸ Michael C. McGarrity, Assistant Director, Counterterrorism Division, Federal Bureau of Investigation, *Confronting White Supremacy*, Statement Before the House Oversight and Reform Committee, Subcommittee on Civil Rights and Civil Liberties, Washington D.C., June 4, 2019, <https://www.fbi.gov/news/testimony/confronting-white-supremacy>.

Islamophobia, and reactions to legislative actions.¹⁹ One development that appears to have impacted both the spread of violent extremism domestically and foreign terrorist organizations' ability to recruit at less expense within the United States, is the increasing use of social media. FBI Director Wray noted that, "Due to online recruitment, indoctrination, and instruction, [foreign terrorist organizations] are no longer dependent on finding ways to get terrorist operatives into the United States to recruit and carry out acts of terrorism."²⁰ He called this trend "a significant transformation from the terrorist threat our nation faced a decade ago."²¹

Some criminologists have referenced a contagion and reinforcement theory wherein past terrorism incidents in a country may have a positive effect on the number of terrorist incidents in the future.²² The FBI noted that the attack at the Chabad of Poway Synagogue in Poway, California, demonstrated the danger presented by the propagation of violent acts on the Internet, adding that the attacker in Poway referenced the mosque attacks in Christchurch, New Zealand, which the latter attacker livestreamed.²³ The FBI noted that they "remain concerned that online sharing of livestreamed attack footage could amplify viewer reaction to attacks and provide ideological and tactical inspiration to other domestic terrorists in the homeland."²⁴ Though the psychological, recruiting, and motivational effects of social media are not per se a financial issue, one could argue that a governmental study of ways to reduce domestic terrorism might benefit from an interdisciplinary—and possibly interagency—approach examining various aspects of technology and social media as they impact domestic terrorism, including financing methods.

Financing of Domestic Terrorism

There is little in the way of public, systematic studies of the financing of domestic terrorism. The Anti-Defamation League (ADL), which examined white supremacy groups in the United States, provides one of the few public sources.²⁵ A 2017 ADL study found that such groups tended to be poorly funded and decentralized rather than highly organized; that they tend to be early adopters of new technologies; they have begun to rely on crowd-funding; and that crowd-funding and use of Bitcoin have become necessary alternatives to credit cards or electronic funds transfer sites, particularly as such groups sporadically are cut off from these payment processors.²⁶ The study flagged the importance of social media, crowd-funding, online lending platforms, and crypto-currencies for these domestic extremists.²⁷ The FBI has also noted that "lone wolf" actors without a clear group affiliation, primarily using firearms, are the

¹⁹ Wray, *Op Cit*.

²⁰ *Ibid*.

²¹ *Ibid*.

²² See, e.g., Midlarsky, M. I., M.Crenshaw, and F. Yoshida, "Why violence spreads—The Contagion of International Terrorism," *International Studies Quarterly*, vol. 24, no. 2, June 1980, pp. 262-298 and Gao, Peng, et al, "Early Detection of Terrorism Outbreaks Using Prospective Space-Time Scan Statistics," *The Professional Geographer*, vol. 65, no. 4, November 2013, https://www.researchgate.net/profile/Peng_Gao27/publication/263183811_Early_Detection_of_Terrorism_Outbreaks_Using_Pro prospective_Space-Time_Scan_Statistics/links/560fd5cd08ae4833751808c5/Early-Detection-of-Terrorism-Outbreaks-Using-Prospective-Space-Time-Scan-Statistics.pdf.

²³ Michael C. McGarrity, Assistant Director, Counterterrorism Division, Federal Bureau of Investigation, *Confronting White Supremacy*, Statement Before the House Oversight and Reform Committee, Subcommittee on Civil Rights and Civil Liberties, Washington D.C., June 4, 2019, <https://www.fbi.gov/news/testimony/confronting-white-supremacy>.<https://www.fbi.gov/news/testimony/confronting-white-supremacy>.

²⁴ *Ibid*.

²⁵ Anti-Defamation League, "Funding Hate: How White Supremacists Raise Their Money," December 5, 2017, <https://www.adl.org/resources/reports/funding-hate-how-white-supremacists-raise-their-money>.

²⁶ See <https://www.adl.org/news/press-releases/hate-groups-increasingly-raising-money-online>.

²⁷ Anti-Defamation League, "Funding Hate: How White Supremacists Raise Their Money," December 5, 2017, <https://www.adl.org/resources/reports/funding-hate-how-white-supremacists-raise-their-money>.

dominant actors in lethal domestic terrorism, and are difficult to identify, investigate, and disrupt.²⁸ This can pose additional challenges in trying to use financing red flags, as such lone perpetrators seem to lack group affiliations, or formally organized resources, and often experience financial strain or have limited means.²⁹ Such self-funded lone-actors can render it challenging to identify patterns of suspicious financial activity related to domestic terrorism, particularly prior to attacks.

Proposals

While the traditional AML/CFT regime in the United States may be effective for combating foreign terrorist organization financing, and sanctioning state sponsors and larger entities,³⁰ it appears that combating the financing of domestic extremists poses novel challenges. One tool the United States has to combat terrorist financing is the collection and analysis of financial data. Evolving technology and use of new data sets (e.g., social media information and electronic payments) may potentially be employed to address those novel challenges. As such, cross-cutting issues that span different areas of congressional oversight may become more important; for example, access to data provided on social media sites and payment platforms. Some argue that expanding data sources examined, including through automated text analysis of social media, and increasing the interoperability of systems that examine the data (such as, between government agencies) can help in identifying domestic terrorists.³¹ Others, however, oppose an expansion of monitoring or surveillance for domestic groups, citing constitutional issues.³²

An approach Congress may choose to pursue is an interdisciplinary, interagency study to examine the use of new technologies in both the spread and financing of domestic terrorism. Such a study may also be used to survey what data sets exist, who has access to that data, and the potential uses of such data. It could also examine other factors in the spread of domestic terrorism, and how to combat it, including but not limited to financing. Legislation introduced in the 116th Congress (H.R. 5132) would require FinCEN to request information from financial institutions for the purpose of developing an advisory about the identification and reporting of suspicious activity related to how “lone wolf” domestic terrorists procure weapons for the purpose of carrying out domestic terror attacks.

Finally, legislation passed by the House in the 116th Congress (H.R. 2513), aimed at increasing transparency of beneficial ownership for entities such as corporations and limited liability corporations (LLCs) may also have value in combating domestic terrorism as well as, more broadly, international terrorism and money laundering. Multiple agencies, including the FBI, have stated that legal entities can be used by hidden owners to raise money, buy assets, or move money anonymously under the current U.S. regime of multiple state laws, which lack a minimum federal identification standard. Opponents of the legislation have asserted that it would burden small businesses and pose privacy concerns for entrepreneurs.³³ On the other hand, multiple agencies have testified it would enable law enforcement to

²⁸ Michael C. McGarrity, Assistant Director, Counterterrorism Division, Federal Bureau of Investigation, *Confronting the Rise of Domestic Terrorism in the Homeland*, Statement Before the House Homeland Security Committee, Washington D.C., May 8, 2019, <https://www.fbi.gov/news/testimony/confronting-the-rise-of-domestic-terrorism-in-the-homeland>.

²⁹ Department of Justice and Federal Bureau of Investigation, *A Study of Lone Offender Terrorism in the United States*, November 2019.

³⁰ This assessment, however, is also debated by scholars; see, e.g., Peter R. Neumann, “Don't Follow the Money: The Problem with the War on Terrorist Financing,” *Foreign Affairs*, July/August 2017, <https://www.foreignaffairs.com/articles/2017-06-13/dont-follow-money..>

³¹ See, e.g., <https://www.nextgov.com/ideas/2018/06/3-ways-use-data-fight-terrorism-and-money-laundering/149043/>.

³² See, e.g., *ACLU Letter to The Senate on the Domestic Terrorism Prevention Act*, S. 894, <https://www.aclu.org/letter/aclu-letter-senate-domestic-terrorism-prevention-act-s-894>.

³³ See <https://www.americanbar.org/content/dam/aba/uncategorized/GAO/2019may6-lettertohofscopposinghr2513substitutebill.pdf>.

more easily trace and monitor assets, including those of domestic terrorists.³⁴ An easier ability to discern underlying owners of corporate entities might offer positive externalities for small business owners as well. For instance, a business owner might more quickly carry out due diligence on prospective borrowers or joint venture partners if he or she had access to information on beneficial owners of legal entities. In short, actions affecting the broader landscape of financial transparency might also help in tracking the financing of domestic terror groups.

³⁴ See, e.g., Kenneth A. Blanco, Director, *Prepared Remarks of FinCEN Director Blanco at the NYU Law Program on Corporate Compliance and Enforcement*, Financial Crime Enforcement Network, June 12, 2019, <https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-blanco-nyu-law-program-corporate-compliance-and>.