

Prepared Remarks of FinCEN Director Andrea Gacki During the SIFMA AML Conference

May 06, 2024

Good morning, it is an honor to join you here today for the first time in my capacity as Director of FinCEN. I very much appreciate SIFMA's invitation to be a part of today's discussion. I had the opportunity to speak with SIFMA's AML Committee earlier this year, and I valued that dialogue and your insights. The perspectives of your industry are incredibly important, particularly given our current priorities.

It is an extremely busy time at FinCEN, so, in our time today, I would like to provide an update on our recent efforts to promote additional transparency in the U.S. financial system; strengthen the U.S. anti-money laundering and countering the financing of terrorism, or AML/CFT, system to align with international standards; and advance the U.S. strategy on countering corruption. Specifically, I'll address our Notice of Proposed Rulemaking for investment advisers, provide an update on FinCEN's efforts to implement the Corporate Transparency Act, and discuss the value of the information that your industry provides to FinCEN and law enforcement, among a few other areas of focus.

Investment Advisers NPRM

As you know, FinCEN issued a proposed rule in February that would require certain investment advisers to implement risk-based AML/CFT programs, report suspicious activity to FinCEN, and fulfill other recordkeeping and reporting requirements.

The investment adviser sector is a key entry point to the U.S. financial system, facilitating the investment of tens of trillions of dollars by individuals, corporations, and retirement plans, among others. Yet investment advisers are not subject to comprehensive AML/CFT regulations in the United States.

We have observed how unscrupulous actors have exploited this sector to access the U.S. financial system for nefarious purposes. We've identified instances in which corrupt officials, tax evaders, other criminals, and sanctioned individuals have gained access to U.S. securities, real estate, and other assets through investment advisers.

These are not new risks. In 2003 and 2015, Treasury proposed applying AML requirements to investment advisers, but those proposed rules were never finalized. Since 2015, the sector has almost doubled in assets under management, and we have developed an increasingly detailed understanding of the illicit finance and national security risks associated with this sector.

Right now, there is a patchwork of regulatory coverage in the investment adviser sector. Certain advisers implement some AML measures because they are dually registered as broker dealers, are affiliated with banks or bank subsidiaries, or are part of a financial holding company already subject to these requirements.

These gaps in regulation allow illicit investors to "shop around" for an adviser who does not need to inquire into their source of wealth. It also creates an unfair playing field in the sector, as different advisers are required to play by different rules.

Alongside the proposed rule, Treasury published a risk assessment specific to the investment adviser sector, which I hope you will find useful. The risk assessment identified several cases where current or former investment advisers laundered illicit proceeds for corrupt foreign officials, fraudsters, and tax evaders.

A FinCEN review of Bank Secrecy Act (BSA) reporting identified several venture capital funds serving as an entry point into the U.S. financial system for Russian oligarchs, and the Office of Foreign Assets Control (OFAC) has several ongoing investigations of sanctions evasion through U.S. venture capital and private funds.

We also identified the extent to which investment advisers and their advised funds, particularly venture capital funds, are being used by foreign states, most notably China and Russia, to access certain technology and services with long-term national security implications through investments in early-stage companies. An analysis of BSA reporting identified several U.S. venture capital firms with significant ties to Russian oligarchs that invested in firms developing emerging technologies with national security applications.

The risk assessment also noted that the highest risk in the investment adviser sector was among exempt reporting advisers, followed by Securities and Exchange Commission (SEC)-registered investment advisers, and then followed by registered investment advisers that are not dually registered as, or affiliated with, a broker-dealer or a bank.

Our current proposal aims to address these risks. We worked hard to tailor the proposal to address national security and illicit finance concerns, while minimizing potential burden on U.S. businesses. We designed the proposed rule to be risk-based, such that smaller advisers may adopt tailored policies and procedures that are consistent with their (often) simpler, more centralized organizational structures.

The proposed rule would also bring the United States into conformity with international standards and address a significant gap in our AML/CFT system identified in the 2016 U.S. mutual evaluation by the Financial Action Task Force (FATF), the international standard-setter for fighting financial crime. The next FATF mutual evaluation of the United States is fast approaching in 2026, and it is important that we move quickly to address this deficiency and remain a global leader in combating money laundering and terrorist financing.

Residential Real Estate

While I am on the subject of proposed rules, our attention is not only on the investment adviser sector. At a time when residential real estate is more expensive than ever and some of our biggest cities are experiencing affordable housing crises, money launderers are exploiting the U.S. housing market and buying homes anonymously to wash their illicitly gained funds. Left unchecked, real estate money laundering can distort housing market prices and make it even more difficult for the average American to afford a home. FinCEN published a notice of proposed rulemaking in February to bring greater transparency to the residential real estate sector that, if finalized, would increase transparency and combat and deter money laundering in the U.S. housing market.

We are also considering next steps with regard to addressing the illicit finance risks associated with the U.S. commercial real estate sector.

The public comments for both the investment adviser and residential real estate proposed rules were robust. We received hundreds of comments, which are under thorough review, and Treasury officials had the opportunity to engage directly with a range of advocacy groups during a series of roundtables on both topics.

Ultimately, hearing a variety of perspectives leads to strong, practical, and effective regulations, and we're looking forward to continuing the rulemaking process to better protect U.S. economic and national security.

Corporate Transparency Act

Another significant priority for FinCEN in our anti-corruption and AML/CFT modernization efforts is our implementation of the Corporate Transparency Act, which requires certain companies doing business in the United States to report their beneficial ownership information to FinCEN. Those requirements went into effect on January 1, 2024, and are commanding a great deal of our attention.

In designing the reporting framework, we worked hard to minimize potential burden on the companies required to report. Filing with FinCEN is simple, secure, and free, and for companies with simple ownership structures, it may only take about 20 minutes. We've already received more than 1.7 million beneficial ownership information reports and are working tirelessly to get the word out to small businesses and their networks.

We're working hard to meet small business owners where they are—by partnering with agencies like the Internal Revenue Service (IRS) and Small Business Administration; publishing multimedia guidance and answers to frequently asked questions, collaborating with secretaries of state; educating trusted service providers like accountants and registered agents; reaching members of trade and industry associations; participating in both in-person and virtual events; and beginning a paid media campaign that encompasses digital, print, radio, streaming, and TV. We're fully committed to ensuring that the filed reports yield a useful database to fulfill the law enforcement and national security purposes laid out in the Corporate Transparency Act.

We are working toward a phased approach to providing access to beneficial ownership information. The first stage will be a pilot program for a handful of key Federal agency users that we expect to begin very soon. The second stage will extend access to Treasury offices and certain Federal agencies engaged in law enforcement and national security activities that already have Memoranda of Understanding for access to BSA information.

Subsequent stages will extend access to additional Federal agencies engaged in law enforcement, national security, and intelligence activities, as well as to State, local, and Tribal law enforcement partners; to intermediary Federal agencies in connection with foreign government requests; and finally, to financial institutions and their supervisors. We expect that financial institutions subject to customer due diligence obligations will receive access in Spring 2025.

AML Act Implementation

Beyond these anti-corruption and transparency efforts, we remain focused on our implementation of the Anti-Money Laundering Act (or, the AML Act). The AML Act included transformational changes to FinCEN's core authorities, with the overall goal of strengthening, modernizing, and streamlining the existing AML regime by promoting innovation, regulatory reform, and industry and stakeholder engagement.

We recognize the importance of full implementation of the AML Act to make the framework more effective and risk-based. The issuance of an updated AML program rule is a foundational part of this effort, and we intend to issue a proposed rule this year that includes regulatory amendments that would ensure that AML/CFT programs incorporate the National AML/CFT Priorities, and are effective, risk-based, and

reasonably designed.

When we issued the Priorities in June 2021, we encouraged financial institutions to assess their risk exposure to those Priorities while we work on implementing regulations. We recognize that financial institutions have been anxiously waiting for a proposed rule to see how they will be required or expected to incorporate the Priorities into their AML/CFT programs.

We view revising the AML/CFT program rule consistently with the AML Act to be a substantial step in a multi-year and multi-step effort to transition to a more effective and risk-based AML/CFT framework.

Russia

In addition to these efforts, FinCEN continues its work across our broad and growing mandate to support law enforcement and national security agencies. First, we are prioritizing the targeting of Russian money laundering and sanctions and export control evasion activities.

In response to Russian's invasion of Ukraine, FinCEN published numerous Alerts to help financial institutions further identify and report suspicious transactions related to potential Russia-related money laundering, and sanctions and export control evasion activities. And we have been analyzing BSA reports filed in response to these Alerts to identify trends and patterns. In September of 2023, FinCEN published a Financial Trend Analysis summarizing some of the findings of that analysis as it relates to BSA reporting related to Russia-related export control evasion. The Alerts and the Financial Trend Analysis are available on our website.

Drawing from that reporting, FinCEN has also been able to conduct and contribute to investigations involving: Russia-related sanctions evasion; violations of the price cap on Russian oil exports; trust and company service providers that obfuscate the wealth of Russian elites; and entities that export dual use technology to Russia's defense sector, the precious metals sector, and Russian private military companies.

Your reporting is providing us with visibility into the financial networks of Russian proliferators, shell companies, fronts, and other professional enablers—leading to new investigations and bolstered existing investigations. These efforts have led to law enforcement actions and civil and administrative actions against a variety of illicit actors. Further, we have partnered particularly closely with OFAC and the Department of Commerce's Bureau of Industry and Security (BIS), which both use BSA data in targeting and enforcement work, and tell us that BSA reports have furthered their ability to leverage their authorities and further disrupt organizations attempting to circumvent Russia-related sanctions.

Countering Russian illicit finance, sanctions and export control evasion, and supporting the U.S. Government's efforts in response to the ongoing war, remain priorities for FinCEN and the Department of the Treasury, and we will continue to evaluate how our tools and authorities can best be utilized in those efforts.

Terrorist Financing

I also want to spend a few moments discussing our efforts to help financial institutions detect, prevent, and report suspicious activity that may be tied to the financing of Hamas and its revenue streams around the world, including entities located in third countries that may be abetting Hamas's fundraising machinations.

The attacks by Hamas against Israel on October 7, 2023, were horrific and only underscored the importance of countering terrorist financing as a core mission of Treasury's Office of Terrorism and Financial Intelligence, including FinCEN.

Shortly after the attack, FinCEN issued an alert containing red flags that FinCEN identified to help financial institutions identify and report suspicious activity connected to funding streams supporting Hamas. Hamas's revenue streams include—or have traditionally included—support from Iran; private donations; a global portfolio of investments; the control of border crossings and avenues of commerce; racketeering business frameworks; extortionary practices around local populations; and fundraising campaigns involving virtual currency and sham charities raising both fiat and virtual currency. Some of those streams have been impacted by the war in Gaza, which Hamas has de facto controlled since 2007.

As a result of this Alert, FinCEN has received over 200 BSA filings. Filers have reported suspicious transactions involving suspected sham charities, potential online fundraising using social media and cryptocurrencies, the purchase of weapons and tactical gear destined for the Middle East, and the use of likely shell companies to obscure the purpose of financial activities.

FinCEN is actively analyzing this information and collaborating with law enforcement and other partners to support investigations and actions to disrupt these terrorist financing networks. Please know that reporting coming in as a result of the Alert will be incredibly valuable to the whole-of-government efforts to deny Hamas the ability to raise funds worldwide for its terrorist activities.

Enforcement and Compliance Efforts

I would now like to turn to some of FinCEN's more recent enforcement and compliance-related work, which has long been a critical component of FinCEN's mission. Those who follow the enforcement space have likely noticed FinCEN becoming increasingly active on these issues, which is consistent with our efforts across various workstreams to increase enforcement by strategically deploying our resources. A significant

component of such efforts is FinCEN's commitment to implementing, and realizing the full potential of, its new Anti-Money Laundering and Sanctions Whistleblower Program.

This program holds tremendous potential as an enforcement force-multiplier. Whistleblowers have submitted information relating to some of the most pressing policy objectives of the United States, from Iran- and Russia-related sanctions evasion to drug-trafficking to cyber-crimes and corruption. While efforts are underway to develop an online tip intake portal and other aspects of this important program, I want to note that even while these efforts are underway, the program is actively receiving, reviewing, and sharing tips with our enforcement partners.

We have received over 270 unique tips since the program's inception, and many of the tips received have been highly relevant to many of Treasury's top priorities. Whistleblowers who voluntarily submit original information to FinCEN about certain violations of the BSA or economic sanctions could be awarded between 10 to 30 percent of penalties collected if their information leads to successful enforcement actions.

I do also want to highlight an action that FinCEN took last November, when FinCEN imposed a landmark \$3.4 billion civil money penalty against Binance, the world's largest virtual asset provider. FinCEN's penalties reflect the breadth and significance of Binance's BSA violations, which included:

1. Failing to Register with FinCEN as a Money Services Business (MSB): Binance claimed to have exited the U.S. market years ago, but did not actually do so, retaining U.S. users and other significant ties with the United States.
2. Failure to Develop, Implement, and Maintain an Effective AML Program: Binance initially failed to develop an AML program, and its subsequent program contained critical gaps that included failing to conduct Know Your Customer processes on large swaths of its users, a lack of risk-based procedures for various offerings, and instructing staff to withhold information from law enforcement.
3. Failure to Report Suspicious Transactions: Binance's lack of AML controls allowed illicit actors to transact freely, supporting activities from child sexual abuse, to illegal narcotics, to terrorism, across more than 100,000 transactions. That includes transactions associated with terrorist groups like Hamas's Al-Qassam Brigades, Palestinian Islamic Jihad, Al Qaeda, and ISIS. Binance processed these transactions, but it never filed a single suspicious activity report (SAR) with FinCEN.

FinCEN's resolution with Binance, along with those of the Commodity Futures Trading Commission, the Department of Justice (DOJ), and OFAC, recognize the role that cryptocurrency companies play in our financial system. As with financial institutions that offer services in fiat currency, willful evasions of U.S. law will be subject to severe repercussions and remediation of the relevant conduct.

Value of BSA Data

I would also like to take some time to share a bit more about what we are seeing in SAR filings by your industry, the value of this information to law enforcement, and the importance of information sharing.

FinCEN received nearly 119,000 SARs from securities and futures filers between April 1, 2022, and March 31, 2024. This averages almost 5,000 SARs a month. Automated Clearing House (ACH) fraud, identity theft, wire transfer fraud, check fraud, and suspicious wire transfers were the most frequently reported suspicious activity subtypes.

Of the top 15 suspicious activity subtypes, the largest percentage increases in reporting from the prior year were for embezzlement, theft, or disappearance of funds—which saw a 34 percent increase—and elder financial exploitation, which increased 63 percent.

Activities most frequently reported in the "other" free text field included "free riding," new account fraud, and money mule schemes.

SAR information is incredibly valuable to law enforcement and other stakeholder for identifying leads and mapping illicit finance networks. Most SARs filed in this time period referenced fraud and/or some form of money laundering activity. About 17 percent mentioned cyber-related terms and about 90 SARs referenced terms related to fentanyl.

In particular, I would like to highlight an investigation that was successful due, in part, to SAR reporting by several broker dealers. This case was the recipient of a FinCEN Law Enforcement Award last year. In this case, the IRS, Criminal Investigation; Federal Bureau of Investigation; and the Small Business Administration Office of Inspector General investigated a massive pandemic relief fraud ring that operated at the height of the COVID-19 pandemic.

The investigation began shortly after the Attorney General's creation of the COVID-19 Fraud Enforcement Task Force. The team was originally tasked with investigating 10 loans made under the Coronavirus Aid, Relief, and Economic Security (CARES) Act of 2020. Investigators quickly used the information found in BSA filings to identify additional fraud and linked the initial list of 10 loans to more than 150 loans totaling approximately \$21 million in fraud.

Because the defendants used fictitious identities and a vast network of bank accounts to commit the fraud and launder the proceeds, investigators also used the public-private information-sharing program FinCEN administers pursuant to section 314(a) of the USA PATRIOT Act to identify additional bank accounts for their investigation. The 314(a) program responses led investigators to additional fraud schemes and, combined with traditional law enforcement tactics, eventually led investigators to the true identity of the culprits. BSA filings were also essential in identifying relationships between co-defendants. Prior to their sentencing, the main defendants fled the United States and became international fugitives.

Again, investigators used BSA data—including SARs filed by broker dealers—to sniff out the financial trail. Investigators were able to run queries through FinCEN's databases and identify accounts that the suspects opened at cryptocurrency exchanges using the same fictitious identities that were used to perpetrate the original fraud. Investigators also discovered that the defendants were applying for additional loans post-indictment and even during trial.

Eventually, the financial trail led investigators to discover the whereabouts of the fugitives. International cooperation resulted in extradition of the defendants. All eight defendants have been sentenced, with the ringleaders receiving sentences of 17 years and nearly 11 years. The U.S. Attorney's Office for the Central District of California, and the DOJ Criminal Division's Fraud Section prosecuted this case.

SAR Tips and Information Sharing

So again, thank you to those broker dealers who helped the investigators piece together and successfully prosecute this case.

Given the high-value of this reporting, I would like to also share some value-creating practices that FinCEN has found increases the value and utility of a financial institution's SARs.

First: Include a "bottom-line-up-front" paragraph at the beginning of each SAR narrative. Clearly identify and explain why the activity is suspicious within the first paragraph of the narrative. This helps law enforcement quickly understand the potential importance and scope of the reported activity and triage its further review and analysis.

Second: Include a citation to – or clear explanation of – the source of any external information triggering the determination that the activity was suspicious. For example, if the triggering event is a press report highlighting a connection to an OFAC sanctioned entity or person, provide a citation to the press report. Or, if the triggering event is consistency with red flags from a FinCEN Alert related to Russia, reference the alert and include the requested keyword in Field 2 and the Narrative. This helps law enforcement understand the full context and identify potential relevance or links to other data sources.

Third: Identify any links to foreign countries, including, for instance, IP addresses. Identifying such links gives FinCEN, as the financial intelligence unit (FIU) for the United States, the opportunity to collaborate with FIUs in other countries, as well as their law enforcement and government partners.

314(b) Program

I do have one last best practice I would like to share, which is really more of a plug for information sharing through our 314(b) program.

I was very encouraged to learn that we currently have approximately 1,700 securities firms already registered to share information under section 314(b) of the USA PATRIOT Act. This comprises over 20 percent of all registered financial institutions and is second only to depository institutions. So, thank you to those who are already registered and actively sharing information under this program.

For those of you who may not be a part of the program, we strongly encourage you to participate and look for opportunities to form associations to engage in voluntary information sharing. And for those already registered, I encourage you to continue to use, and potentially expand, existing processes to collect and share information in furtherance of investigations that involve cross-border activity.

FinCEN truly views information sharing as one of the most powerful tools to help enhance compliance with AML/CFT requirements.

One of the most valuable uses of 314(b) information sharing is alerting other participating financial institutions to customers whose suspicious activities they may not have been previously aware. Relatedly, 314(b) information sharing facilitates the filing of more comprehensive SARs than would otherwise be filed.

In cases where a financial institution files a SAR that has benefited from section 314(b) information sharing, FinCEN encourages financial institutions to note this in the narrative. Doing so not only provides useful context for law enforcement, it also helps FinCEN identify and communicate specific examples of the benefits of the section 314(b) program.

To that end, FinCEN updated its SAR User Guide in August 2021 to request financial institutions include the sentence "This SAR contains 314(b) data." in the narrative for such cases. The most up-to-date version of this user guide can always be found on our BSA E-Filing website.

Conclusion

I know I have covered quite a bit of ground today in our time together, but I believe it speaks to the broad scope of FinCEN's mission and the range of functions that FinCEN performs as we work to address the various illicit finance threats facing our country. In some ways, I feel like I just scratched the surface, and to that end, you will be hearing more from my FinCEN colleagues today on both the enforcement and CTA panels.

Thank you again and enjoy the rest of the conference.

###



[Home \(/\)](#)

[Resources \(/resources\)](#)

[Contact \(/contact\)](#)

[About \(/what-we-do\)](#)

[Careers \(/cutting-edge-opportunities\)](#)

[Newsroom \(/news-room\)](#)

[Contract Opportunities \(/about/contract-opportunities\)](#)

[Get News Updates \(https://service.govdelivery.com/accounts/USFINCEN/subscriber/new\)](https://service.govdelivery.com/accounts/USFINCEN/subscriber/new)

<https://www.facebook.com/fincentreasury><https://www.linkedin.com/company/fincen><https://twitter.com/FinCENnews><https://www.youtube.com/@fincentreasury>

[USA.gov \(https://www.usa.gov\)](https://www.usa.gov) | [Regulations.gov \(https://www.regulations.gov\)](https://www.regulations.gov) | [Treasury.gov \(https://www.treasury.gov\)](https://www.treasury.gov) | [IRS.gov \(https://www.irs.gov\)](https://www.irs.gov) | [Freedom of Information Act \(FOIA\) \(/freedom-information-act-foia-and-guide-accessing-fincen-information\)](#) | [NO FEAR Act \(https://home.treasury.gov/footer/no-fear-act\)](https://home.treasury.gov/footer/no-fear-act) | [Vote.gov \(https://vote.gov/\)](https://vote.gov/) | [Accessibility \(/accessibility\)](#) | [EEO & Diversity Policy \(/equal-employment-opportunity-and-diversity-policy\)](#) | [Privacy Policy \(/privacy-security\)](#) | [Public Posting Notice of Finding of Discrimination \(https://home.treasury.gov/footer/no-fear-act\)](https://home.treasury.gov/footer/no-fear-act) | [Security and Vulnerability Disclosure Policies \(VDP\) \(/security-and-vulnerability-disclosure-policies\)](#) | [Office of Inspector General \(https://oig.treasury.gov/\)](https://oig.treasury.gov/)