ACAMS

Anti-Financial Crime Briefing

DeFi and Anti-Money Laundering

Background

Despite recent market turmoil, decentralized finance (DeFi) exists as an emerging technology class that must be understood by the financial crime compliance community. Anti-money laundering (AML) risks remain an underexplored topic surrounding DeFi, so this brief will focus exclusively on recent developments in AML and DeFi.[1]

Innovation continues to drive new technologies and products in financial services, such as the development of DeFi protocols for cryptoassets. DeFi proponents seek to reduce costs for financial transactions, increase market efficiency and transparency, and dislodge traditional financial intermediaries, including through permissionless and decentralized transactions. DeFi critics and skeptics view the technologies as perpetuating or exacerbating existing risks and vulnerabilities, especially to retail customers and market integrity, while often lacking actual decentralization of business operations.

Non-financial crime related enforcement activity has been undertaken (or is ongoing) by a range of agencies against a variety of centralized and decentralized entities, including companies, developers, and non-regulated enablers (including a cryptoasset mixing service). This demonstrates that regulators are seeking to bring DeFi into the regulatory perimeter and will act against rogue actors. Controlling or accountable operators must already comply with existing obligations, such as abiding by Office of Foreign Assets Control (OFAC) administered economic sanctions. As DeFi protocols continue to be exploited by criminal actors and are met with further enforcement activity, DeFi actors and counterparties with exposure to DeFi are likely to be subject to further regulatory monitoring including, but not limited to, enhanced financial crime rules and regulations.

Relevance

How does this relate to AML compliance?

- The use of DeFi protocols for financial transactions raises both novel and old questions about how to apply AML requirements. DeFi's focus on permissionless and decentralized financial transactions tests a central feature of AML policy and regulatory architecture, that generally relies on financial institution intermediaries for customer due diligence including know your customer (KYC), record keeping, and reporting like filing suspicious activity reports (SARs). Policymakers continue to recognize that heightened AML compliance obligations do not apply to software, but not all activities self-branded as "DeFi" may benefit from this exemption.

1. This brief will not focus on countering the financing of terrorism (CFT); rather, CFT is incorporated by reference to AML in this brief. The United States has assessed that while terrorists have used cryptoassets, the overall terrorist use of cryptoassets "appears to remain limited when compared to other financial products and services" with no specific assessment of DeFi. See U.S. Department of the Treasury, February 2022, "2022 National Terrorist Financing Risk Assessment", at 22, **https://home.treasury.gov/system/files/136/2022-National-Terrorist-Financing-Risk-Assessment.pdf**.

- AML risks exist within the DeFi ecosystem. The Financial Action Task Force (FATF) – the intergovernmental AML/CFT standard-setting body – recently found that "DeFi is increasingly used for money laundering" based on open-source information from a blockchain analytics company.[2] The US government found, for instance, that DeFi applications have converted the illicit proceeds of ransomware-related payments.[3] A blockchain analytics firm found that DeFi users and investors lost more than US$10.5 billion due to theft and fraud in 2021 (as of November), and US$1.5 billion in 2020.[4] AML risks appear to be increasing over time as DeFi becomes more widely adopted.
- Other features of cryptoassets that apply equally to DeFi transactions may improve AML compliance. The public design of blockchains with immutable public ledgers are features that do not exist with other financial transactions, thereby providing compliance professionals, counterparties, regulators, and law enforcement with new tools for blockchain and transaction analytics.
- Even where US Bank Secrecy Act (BSA) AML requirements may not apply to DeFi activities, all US persons, and some non-US persons, must comply with existing US economic sanctions laws and regulations. This compliance obligation can create DeFi protocol, counterparty, and liquidity provider risk.

Context

What is DeFi?

DeFi lacks a common definition. The Bank of England's Financial Policy Committee defines DeFi as "a collective term for a set of applications that seek to provide a range of financial services, including loans and exchanges, with the aim of reducing reliance on centralized financial intermediaries. These alternative financial applications are built on distributed ledger technology. Unlike traditional financial services firms that undertake these activities, DeFi applications are, at present, largely unregulated."[5] Most DeFi applications today are built on the Ethereum blockchain.[6]

Importantly from a definitional and financial crimes compliance perspective, FATF found that "recent outreach with industry suggests that 'decentralized' currently can be a marketing term rather than a technical description, and that even in so-called decentralized arrangements, often there continues to be persons and centralized aspects that may be subject to AML/CFT obligations."[7]

However, the U.S. Treasury Department stated that DeFi "refers to a class of virtual asset protocols and platforms, some of which allow for automated [peer-to-peer] transactions without the need for an account or custodial relationship and often through the use of smart contracts."[8]

2. Financial Action Task Force, June 2022, "Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers", at 19, **https://www.fatf-gafi.org/publications/fatfrecommendations/documents/targeted-update-virtual-assets-vasps.html**.
3. U.S. Department of the Treasury, Financial Crimes Enforcement Network, October 2021, "Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021", at 13, **https://www.fincen.gov/sites/default/files/2021-10/Financial Trend Analysis_Ransomware 508 FINAL.pdf**.
4. Elliptic, November 18, 2021, "DeFi: Risk, Regulation, and the Rise of DeCrime", **https://www.elliptic.co/resources/defi-risk-regulation-and-the-rise-of-decrime**.
5. Bank of England Financial Policy Committee, March 2022, "Financial Stability in Focus: Cryptoassets and decentralised finance", **https://www.bankofengland.co.uk/-/media/boe/files/financial-stability-in-focus/2022/cryptoassets-and-decentralised-finance.pdf**.
6. Alyssa Hertig, CoinDesk, Updated May 24, 2022, "What is DeFi?", **https://www.coindesk.com/learn/what-is-defi/**.
7. Financial Action Task Force, June 2022, at 3, Op. Cit.
8. U.S. Department of the Treasury, February 2022, "National Money Laundering Risk Assessment", at 42, **https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf**

Even proponents of, and investors in, DeFi have identified the core challenge of DeFi and AML: "The very nature of decentralized finance on public blockchains like Ethereum is to facilitate permissionless exchange, but this open access is generally incompatible with anti-money laundering/combating the financing of terrorism (AML/CFT) regulations as currently implemented in the US."[9]

DeFi and stablecoins

DeFi must also be understood in the context of **stablecoins**.[10] FATF found in June 2022 that "the increasing use of stablecoins in DeFi protocols commensurate with growth in the DeFi market" was a "notable change" in the DeFi market over the past year.[11] According to U.S. Treasury Department Under Secretary for Domestic Finance Nellie Liang, stablecoins support the "functioning of decentralized finance."[12] According to the New York Times, "Stablecoins are a critical part of DeFi markets, because if you're a crypto investor, you don't want to constantly be changing tokens back and forth to dollars, or keeping all your assets in cryptocurrencies whose values might fluctuate wildly."[13]

International financial crimes policy approach to DeFi

Most recently, on June 30, 2022, FATF published a targeted update on implementation of its standards on cryptoassets, which they call virtual assets (VA) and virtual asset service providers (VASPs). FATF acknowledged that member countries and the private sector "identify DeFi and [non-fungible tokens] as a challenging area for implementation of the FATF Standards."[14]

Importantly, FATF reiterated its October 2021 guidance that the FATF Standards do not apply to software.[15] However, FATF qualified this position by stating that "Nonetheless, the FATF Standards can apply to persons who maintain control or sufficient influence over a DeFi arrangement or protocol providing VASP services."[16]

In concluding its analysis of DeFi, FATF committed to "continuing to monitor developments in DeFi, particularly the emergence of truly decentralized DeFi entities, and to facilitate dialogue on common AML/CFT implementation challenges, risk assessment, and good practices."[17]

The Bank for International Settlements (BIS) – the central bank to global central banks – takes a highly skeptical view of DeFi in general while also raising AML concerns. The BIS experts have stated: "The limited application of anti-money laundering and know your customer (AML/KYC) provisions, together with transaction anonymity, exposes DeFi to illegal activities and market manipulation."[18]

Other international organizations have identified non-AML but related risks from DeFi, such as cybersecurity. The International Monetary Fund (IMF) called cyberattacks "lethal" for DeFi platforms because they "steal financial assets and undermine user trust."[19]

9. Nic Carter and Linda Jeng, RegTech, SupTech and Beyond: Innovation and Technology in Financial Services, August 6, 2021, "DeFi Protocol Risks: The Paradox of DeFi", at 30, available at: **https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3866699**.
10. See ACAMS Stablecoin Rapid Response Brief: **https://www.acams.org/en/media/document/30786**.
11. Financial Action Task Force, June 2022, at 19, Op. Cit.
12. U.S. Department of the Treasury, November 1, 2021, "Remarks by Under Secretary for Domestic Finance Nellie Liang to the Stanford Graduate School of Business", **https://home.treasury.gov/news/press-releases/jy0455**.
13. Kevin Roose, The New York Times, March 18, 2022, "What is DeFi?", **https://www.nytimes.com/interactive/2022/03/18/technology/what-is-defi-cryptocurrency.html**.
14. Financial Action Task Force, June 2022, at 19, Op. Cit.
15. Ibid.
16. Ibid.
17. Ibid. at 20, emphasis in original.
18. Sirio Aramonte, Wenqian Huang, and Andreas Schrimpf, Bank for International Settlements, BIS Quarterly Review, December 6, 2021, "DeFi risks and the decentralisation illusion", **https://www.bis.org/publ/qtrpdf/r_qt2112b.htm**.
19. Antonio Garcia Pascual and Fabio Natalucci, International Monetary Fund, April 13, 2022, "Fast-Moving FinTech Poses Challenge for Regulators", **https://blogs.imf.org/2022/04/13/fast-moving-fintech-poses-challenge-for-regulators/**.

DeFi and US responsible innovation policy

President Biden's March 9, 2022, Executive Order on Ensuring Responsible Development of Digital Assets identified DeFi, mostly in the context of illicit finance risks.[20] The overarching Biden Administration policy is to "mitigate the illicit finance and national security risks posed by misuse of digital assets." This framing importantly acknowledges the licit uses of cryptoassets by focusing policy attention on misuse, rather than, for instance, broadly claiming that all cryptoassets pose illicit finance and national security risks.

The Executive Order noted: "Growth in decentralized financial ecosystems, peer-to-peer payment activity, and obscured blockchain ledgers without controls to mitigate illicit finance could also present additional market and national security risks in the future."[21] To counter these risks, the Executive Order laid out US policy to focus on controls and accountability: "The United States must ensure appropriate controls and accountability for current and future digital assets systems to promote high standards for transparency, privacy, and security – including through regulatory, governance, and technological measures – that counter illicit activities and preserve or enhance the efficacy of our national security tools."[22]

The U.S. Treasury Department recently committed to monitor "decentralized finance platforms and applications" for illicit activity as part of its 2022 National Strategy for Combating Terrorism and Other Illicit Financing.[23]

The evolving FinCEN approach to DeFi

The Treasury Department's Financial Crimes Enforcement Network (FinCEN) is the US government's lead AML financial regulator, with oversight of DeFi activities that trigger AML regulatory obligations equivalent to other covered financial institutions.[24]

In 2019, FinCEN released updated guidance on what the agency calls "convertible virtual currencies (CVCs)".[25] The 2019 FinCEN Guidance addresses a range of activities related to cryptoassets and DeFi, including distributed applications (DApps) and decentralized exchanges (DExs). According to FinCEN, "a person is exempt from money transmitter status if the person only provides the delivery, communication, or network access services used by a money transmitter to support money transmission services."[26] Relatedly, the 2019 FinCEN Guidance also importantly addressed the regulatory treatment of certain financial intermediaries for CVC wallets based on four criteria: "a) who owns the value; b) where the value is stored; c) whether the owner interacts directly with the payment system where the CVC runs; and d) whether the person acting as intermediary has total independent control over the value."[27]

The 2019 FinCEN Guidance built on a decade of work by the bureau to bring new and emerging cryptoassets into a regulatory framework for AML/CFT. In 2011, FinCEN issued a final rule that modified the definition of a money services business (MSB) under the Bank Secrecy Act (BSA) and importantly addressed "other value that substitutes for currency" when defining "money transmission services."[28] In 2013, FinCEN released guidance on the

20. The White House, March 9, 2022, "Executive Order on Ensuring Responsible Development of Digital Assets", **https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/**.
21. Ibid.
22. Ibid.
23. U.S. Department of the Treasury, May 2022, "National Strategy for Combating Terrorist and Other Illicit Financing", at 12, **https://home.treasury.gov/system/files/136/2022-National-Strategy-for-Combating-Terrorist-and-Other-Illicit-Financing.pdf**.
24. U.S. Department of the Treasury, Financial Crimes Enforcement Network, "About Us: Mission", **https://www.fincen.gov/about/mission**.
25. U.S. Department of the Treasury, Financial Crimes Enforcement Network, May 9, 2019, "FinCEN Guidance: FIN-2019-G001 Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies", **https://www.fincen.gov/sites/default/files/2019-05/FinCEN Guidance CVC FINAL 508.pdf**.
26. Ibid. at 24.
27. Ibid. at 15.
28. Code of Federal Regulations, 31 CFR 1010.100(ff)(5)(i)(A), **https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1010#p-1010.100(ff)(5)(i)(A)**.

applicability of FinCEN's regulations to those administering, exchanging, or using virtual currencies.[29] Determining whether a DeFi protocol has a BSA AML obligation can turn on whether the protocol is operating as an MSB.[30]

Industry advocates for DeFi have taken the position that "non-custodial DeFi protocols are not subject to the BSA framework and its reporting requirements" because "whenever individual users interact with a DeFi protocol to conduct a financial activity, those users have custody and control over their assets, and they act on their own behalf."[31]

Economic sanctions considerations

Even where BSA AML requirements do not apply, US economic sanctions compliance obligations exist for all US persons as well as certain non-US persons. US economic sanctions are administered by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC).

OFAC continues to focus its sanctions designations, compliance, and enforcement efforts in the cryptoassets space:

- In 2022, OFAC designated the first virtual currency mining company, Bitriver AG, along with multiple subsidiaries[32]
- In 2021, OFAC designated its first two virtual currency exchanges, Suex and Chatex[33]
- In 2020 and 2021, OFAC published guidance related to ransomware that involves cryptoassets[34]
- In 2021, OFAC issued specific guidance for the convertible virtual currency (CVC) industry[35]
- In 2020 and 2021, OFAC's Enforcement Division entered into settlements with cryptoasset companies BitGo and BitPay, respectively, for apparent violations related to cryptoasset transactions[36]

DeFi investors and proponents have themselves identified the sanctions risks posed by DeFi. Using the example of a Uniswap liquidity pool, "If some tainted liquidity, for instance emanating from an OFAC-sanctioned party or an illicit source, were to enter a Uniswap pool, regular users would effectively be undertaking a financial relationship with these prohibited parties. As currently deployed, the smart contract has no means to whitelist users or permission them a *priori*."[37] Other DeFi industry advocates have catalogued the steps taken by DeFi protocols to comply with sanctions obligations, including through geofencing and wallet screening using blockchain analytics tools.[38]

29. U.S. Department of the Treasury, Financial Crimes Enforcement Network, March 18, 2013, "Guidance FIN-2013-G001 Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies", **https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf**.
30. Ari Redbord, ACAMS Today, March 17, 2022, "DeFi Compliance: A Galaxy Not Far Away", **https://www.acamstoday.org/defi-compliance-a-galaxy-not-far-away/**.
31. Defi Education Fund, February 18, 2022, "AML/CFT Part 1: Where Government Meets DeFi", **https://medium.com/@defieducationfund/aml-cft-part-1-where-government-meets-defi-3bf15e33f8a5**.
32. U.S. Department of the Treasury, April 20, 2022, "U.S. Treasury Designates Facilitators of Russian Sanctions Evasion", **https://home.treasury.gov/news/press-releases/jy0731**.
33. U.S. Department of the Treasury, September 21, 2021, "Treasury Takes Robust Actions to Counter Ransomware", **https://home.treasury.gov/news/press-releases/jy0364**; U.S. Department of the Treasury, November 8, 2021, "Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange", **https://home.treasury.gov/news/press-releases/jy0471**.
34. U.S. Department of the Treasury, September 21, 2021, "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments", **https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf**.
35. U.S. Department of the Treasury, October 15, 2021, "Publication of Sanctions Compliance Guidance for the Virtual Currency Industry and Updated Frequently Asked Questions", **https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20211015**.
36. U.S. Department of the Treasury, December 30, 2020, "Enforcement Release: OFAC Enters Into $98,830 Settlement with BitGo, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions", **https://home.treasury.gov/system/files/126/20201230_bitgo.pdf**; U.S. Department of the Treasury, February 18, 2021, "Enforcement Release: OFAC Enters Into $507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions", **https://home.treasury.gov/system/files/126/20210218_bp.pdf**.
37. Nic Carter and Linda Jeng, 29-30, Op. Cit.
38. DeFi Education Fund, March 3, 2022, "AML/CFT Part 2: Sanctions Compliance and Law Enforcement in the Defi Ecosystem", **https://medium.com/@defieducationfund/aml-cft-part-2-sanctions-compliance-and-law-enforcement-in-the-defi-ecosystem-22fda78e4cc6**.

Enforcement activities

The Treasury Department, through OFAC and FinCEN, has not yet sanctioned or taken an enforcement action against a DeFi protocol. Therefore, it is instructive to understand related enforcement actions taken by other financial regulators to date.

The U.S. Securities and Exchange Commission (SEC) took its first action against two American individuals, Gregory Keough and Derek Acree, and Blockchain Credit Partners (d/b/a DeFi Money Market), their Cayman Islands company, for more than US$30 million in unregistered sales of securities that used smart contracts and DeFi technology.[39] While this cease and desist proceeding by the SEC administrative panel did not directly involve allegations of money laundering, the SEC's action does signal regulatory enforcement interest and capability to target the DeFi ecosystem.

On January 3, 2022, the U.S. Commodity Futures Trading Commission (CFTC) entered an order and settled charges against Blockratize (d/b/a Polymarket), a DeFi betting platform that failed to register with the CFTC.[40] Polymarket used smart contracts hosted on a blockchain to manage the bets.

Public reports also indicate that the SEC opened an investigation into Uniswap Labs, the software developer behind a prominent DeFi cryptoasset exchange.[41] The investigation addresses the use and marketing of the protocol but further indicates regulatory enforcement interest in DeFi protocols.

Practical Steps for Compliance

- Review current FATF, FinCEN, and OFAC cryptoasset guidance, as well as state-level guidance, including the recent New York Department of Financial Services **Virtual Currency Guidance** on blockchain analytics.
- For covered US financial institutions subject to the Bank Secrecy Act, implement relevant FinCEN guidance, including the 2019 FinCEN Guidance on cryptoassets.
- For DeFi protocols not subject to the Bank Secrecy Act, develop and implement economic sanctions compliance programs consistent with applicable OFAC regulations and guidance, as well as industry best practices such as geofencing and blockchain analytics.
- Monitor negative news for DeFi hacks, exploits, and other risks to financial markets.
- Analyze DeFi protocols to determine which are truly decentralized or are merely using "decentralized" for marketing or branding purposes.

39. U.S. Securities and Exchange Commission, August 6, 2021, "SEC Charges Decentralized Finance Lender and Top Executives for Raising $30 Million Through Fraudulent Offerings: Case is Agency's First Involving Securities Using DeFi Technology", **https://www.sec.gov/news/press-release/2021-145**.
40. Commodity Futures Trading Commission, January 3, 2022, "Release Number 8478-22: CFTC Orders Event-Based Binary Options Markets Operator to Pay $1.4 Million Penalty", **https://www.cftc.gov/PressRoom/PressReleases/8478-22**.
41. Dave Michaels and Alexander Osipovich, The Wall Street Journal, September 3, 2021, "Regulators Investigate Crypto-Exchange Developer Uniswap Labs", **https://www.wsj.com/articles/regulators-investigate-crypto-exchange-developer-uniswap-labs-11630666800**.

Authors

Justine Walker, Global Head of Sanctions, Compliance and Risk

Joby Carpenter, Subject Matter Expert, Cryptoassets and Emerging Threats

Developed in partnership with **Alex Zerden**, ACAMS co-opted expert/Adjunct Senior Fellow, Center for a New American Security

August 3, 2022

Disclaimer

The content contained herein is for general information purposes only and is neither legal nor business advice. You should consult your own legal and business advisors for advice that applies to your situation.

About ACAMS

ACAMS is the largest international membership organization dedicated to providing opportunities for anti-financial crime (AFC) education, best practices, and peer-to-peer networking to AFC professionals globally. With over 90,000 members across 180 jurisdictions, ACAMS is committed to the mission of ending financial crime through the provision of anti-money laundering/counter-terrorism financing and sanctions knowledge-sharing, thought leadership, risk-mitigation services, ESG initiatives, and platforms for public-private dialogue. The association's CAMS certification is the gold-standard qualification for AFC professionals, while the CGSS certification is its premier specialist qualification for sanctions professionals. ACAMS' 60 Chapters globally further amplify the association's mission through training and networking initiatives.

For more resources on topical anti-financial crime issues, visit the ACAMS Insights hub: **www.acams.org/insights**