J5 JOINT CHIEFS OF GLOBAL TAX ENFORCEMENT

Law Enforcement Advisory Report

Over-The-Counter Cryptocurrency Trading Desks

01
26

The Emerging Threat of Cryptocurrency Trading Desks

Over-The-Counter (OTC) cryptocurrency trading desks act as intermediaries between individual buyers and sellers who, for various reasons, choose not to or cannot transact on an open exchange. OTC clients seek to quickly and easily buy or sell large amounts of digital assets. They may include high net worth individuals, institutions, venture capital (VC) firms, and hedge funds who invest in cryptocurrency markets. OTC desks provide clients with anonymity and reliability when moving large sums of money and cryptocurrency, thus potentially functioning as an obfuscation tool for tax evaders and money launderers.

OTC desks often operate in coordination with liquidity providers (LPs), which are entities or individuals that supply large amounts of digital assets to facilitate trades. These liquidity providers play a crucial role in ensuring that transactions are executed efficiently, particularly in volatile or illiquid markets. Together, OTC desks and liquidity providers account for a large share of cryptocurrency trading activity. Recent estimates suggest that OTC transactions represent the majority of volume in the digital asset market, with trillions of dollars in trades occurring annually across numerous jurisdictions.

Desired Features: Privacy & Anonymity

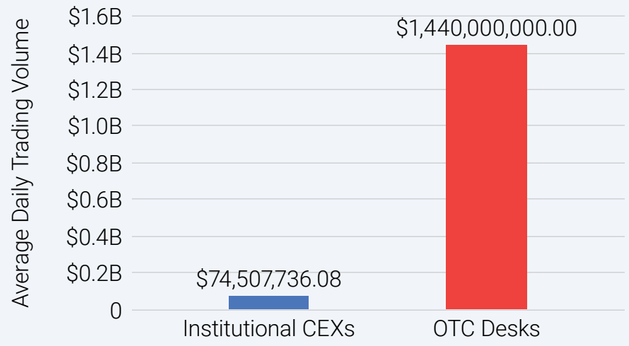
OTC desks provide anonymity that is not generally available on centralized cryptocurrency exchanges (CEXs). The privacy provided by OTC desks to their clients makes it difficult to ascertain who is using their services.

Unlike CEXs, OTC desks often cater to high-net worth traders. Independent buyers and sellers are often required to trade at the industry minimum of $50,000 U.S. dollars (USD) equivalent.[1] [2] While there are legitimate uses for OTC desks, they may also be used for illicit purposes such as tax evasion, money laundering, sanctions evasion, or other unlawful activities.

Money Laundering Risks: Bypassing Anti-Money Laundering (AML) Controls

Law enforcement and regulatory agencies are not able to monitor in real time the billions in cryptocurrency assets that are moved daily by OTC desks as many of the OTC desks are not identified and labeled in many of the widely used commercial blockchain analysis tools. In addition, OTC desk transactions often occur internally and are not visible on the publicly available blockchain.

Average Daily Trading Volumes, 2023
Institutional CEXs vs OTC Desks



Source: CCData and Finery Markets

Despite facilitating billions in daily transactions, the majority of OTC desks may not be filing suspicious activity reports (SARs) to mitigate the risks associated with the sheer volume of cryptocurrency being exchanged.[3] As a result, OTC desks may be providing an added layer for criminal actors seeking to launder illicit funds from the cryptocurrency ecosystem into traditional finance.

THREATS (CONTINUED)

[1] help.crypto.com: What is the Over-the-Counter (OTC) Trading Service? https://help.crypto.com/en/articles/5733702-what-is-otc-trading

[2] All dollar amounts in this report are USD.

[3] SARs are the U.S. and U.K. equivalents of Suspicious Transaction Reports (STRs) in Canada and the Netherlands and Suspicious Matter Reports (SMRs) in Australia.

The Emerging Threat of Cryptocurrency Trading Desks (continued)

Rising Trend: SARs

SARs filed with the Financial Crimes Enforcement Network (FinCEN) involving cryptocurrency OTC desks and liquidity providers have increased over the past several years.

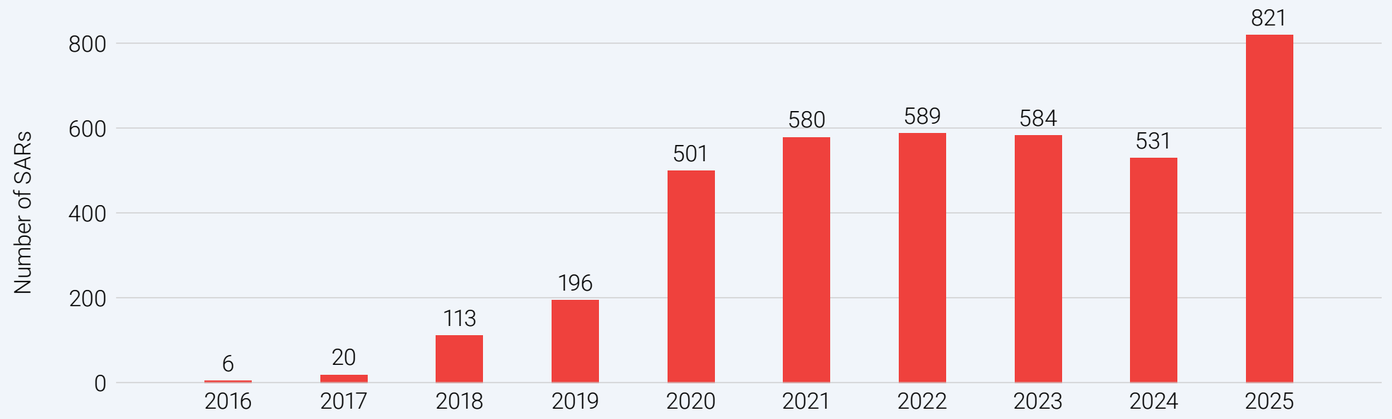
While these entities were initially used to facilitate digital asset trades, they are now also being used to move large amounts of value in ways that may conceal the origin of funds. This shift suggests a broader role in layering and other forms of obfuscation.

From 2016 through 2019, SAR filings remained relatively low but rose steadily each year. The trajectory since then has shown a substantial increase in reporting, with filings totaling 501 in 2020 and 580 in 2021. While the SAR reporting remained stable within the 500 range through 2024, the filings increased to a new peak of 821 in 2025.

This upward trend reflects both the growing use of OTC desks and liquidity providers and closer scrutiny by financial institutions.

To date, approximately $235 billion in suspicious activity has been reported to FinCEN in connection with these platforms. These filings provide law enforcement with useful data to identify patterns, assess risks, and pursue investigations into potential misuse in the digital asset space.

Number of SARs Filed with FinCEN Related to Cryptocurrency OTC Desks from 2016 through 2025



Source: FinCEN Data from 2016 through 2025

Sum	Average	Min	Max
$235,806,377,636	$61,216,608.94	$0	$27,712,606,679

Source: FinCEN Data from 2016 through 2025

The trend of increasing SARs provides law enforcement an opportunity to dive deeper into the reported data, enabling the identification and targeting of OTC desks and liquidity providers that may be associated with various illicit activities.

THREATS (PREVIOUS)

Enhancing Law Enforcement Strategies

The Joint Chiefs of Global Tax Enforcement (J5) emphasizes the importance of law enforcement agencies reviewing financial intelligence unit (FIU) data with the focus on the emerging industry of OTC desks and liquidity providers. Specific keyword searches can help identify SAR narratives that detail alledged instances of tax evasion, money laundering, or other financial crimes facilitated by OTC desks.

Effective use of FIU data and targeted searches can aid law enforcement in identifying potential leads for investigation, disrupting illegal activities, developing intelligence of emerging threats and trends, and enhancing their understanding of the cryptocurrency landscape and its vulnerabilities.

Leveraging Targeted FIU Searches

Some of the best practices for targeting potential illicit activity involving cryptocurrency OTC desks include creating search terms using synonyms like “cryptocurrency,” “virtual assets,” “digital assets,” and “digital currency” to capture different terminology used by financial institutions reporting SARs. By combining these terms with OTC-related keywords such as “over-the-counter,” “OTC desk,” “trading desk,” or “liquidity provider,” law enforcement can focus on specific SARs.

These searches can help identify suspicious transactions or patterns indicative of tax evasion or money laundering, identify individuals or entities using cryptocurrency OTC desks to circumvent reporting requirements, and disrupt tax evasion and money laundering using OTC desks and liquidity providers.

Targeted Keyword Searches for Cryptocurrency OTC Trading Desk SARs

1. Crypto OTC
2. Crypto Over the Counter
3. Crypto Trading Desk
4. Crypto Trading Firm
5. Crypto Trading Platform
6. Crypto Liquidity Provider

Note: The recommendations are meant to be used in conjunction with other investigative techniques and tools and should be tailored to the specific needs of the agency.

Protecting the Financial System

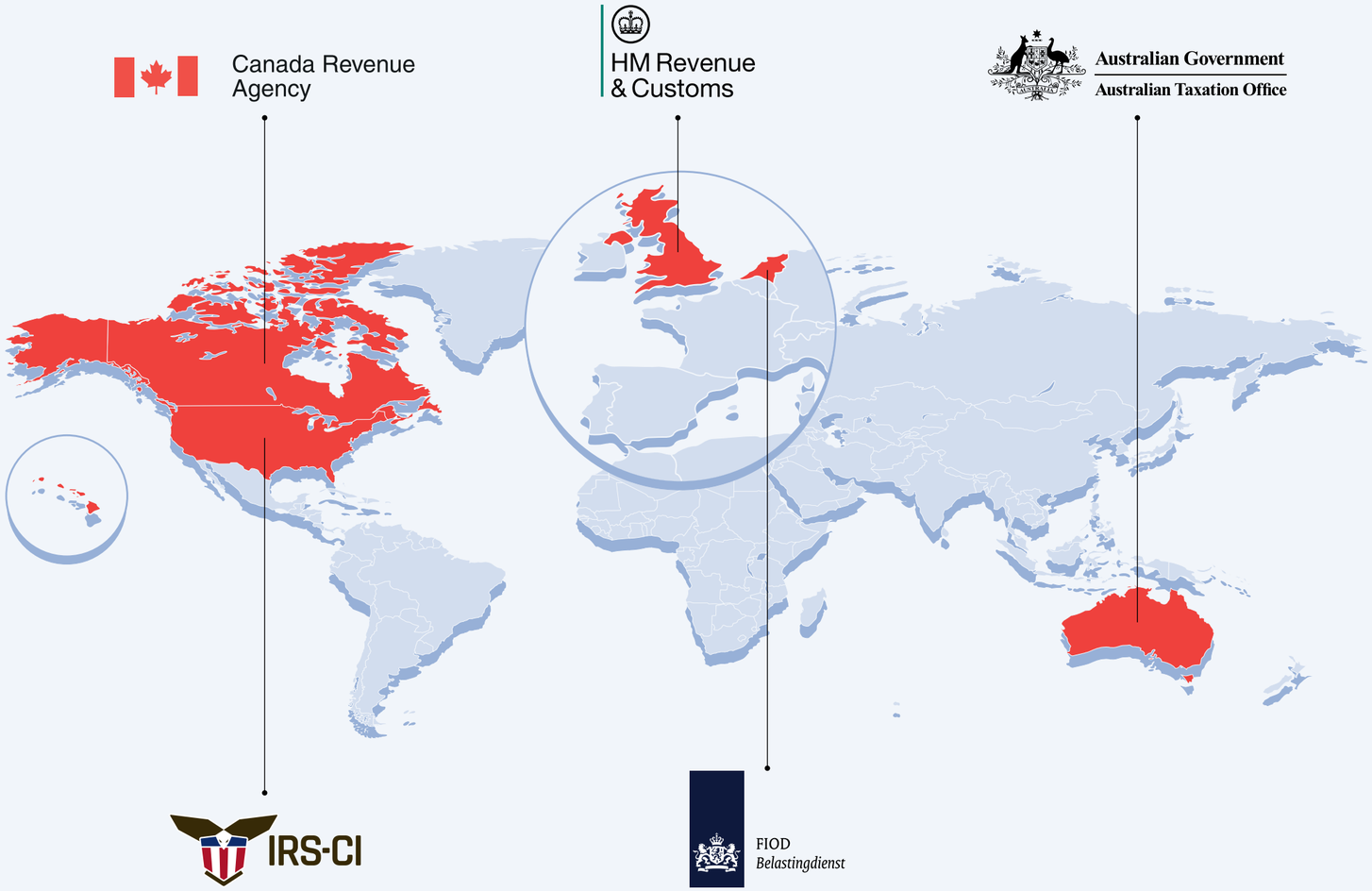
The rise of cryptocurrency OTC desks and liquidity providers poses significant risks and novel threats to the integrity of the global financial system. While the United States’ Bank Secrecy Act requires anti-money laundering compliance programs, the ease in which vast amounts of illicit funds can be laundered through these platforms has provided a new platform for criminals to further obscure their financial activities. This J5 report provides insights to enhance the detection of tax evasion and money laundering by understanding the risks associated with cryptocurrency OTC desks and liquidity providers. The use of targeted SAR search words enables law enforcement and FIUs to conduct more effective investigations. By working together and sharing intelligence, the J5 combats financial crime and promotes tax compliance in the evolving digital asset landscape.

About the J5

The J5 leads the fight against international tax crime and money laundering, including digital asset threats and those who undertake, enable, or facilitate global tax evasion. The J5 works together to gather information, share intelligence, and conduct coordinated operations against transnational financial crimes. The J5 includes the Australian Taxation Office, the Canada Revenue Agency, the Dutch Fiscal Intelligence and Investigation Service, His Majesty's Revenue and Customs from the U.K. and IRS Criminal Investigation from the U.S.

The J5 Cyber Group seeks to identify and work the largest, most impactful digital assets related cybercrime investigations in the world related to tax evasion, money laundering, and other related financial crime. Inquiries and tips can be sent to J5Cyber@ci.irs.gov.

For more information about the J5, please visit j5alliance.global.



J5 JOINT CHIEFS OF GLOBAL TAX ENFORCEMENT

1-2026