# DOJ sharpens its cryptocurrency enforcement focus

**By Daniel L. Stein, Esq., Glen A. Kopp, Esq., and Brendan J. Harrington, Esq., Mayer Brown**

**NOVEMBER 30, 2021**

Since its inception, cryptocurrency has been the subject of hot debate. Proponents of more widespread use and investment see tremendous potential for a decentralized but secure medium of exchange with untold implications for global finance. Detractors instead argue that cryptocurrency is highly volatile, inconvenient, and designed to facilitate illegal conduct. One thing all can agree on, however, is that the U.S. Department of Justice (DOJ) is sharpening its focus on combatting cryptocurrency-related crimes.

*The NCET will not only investigate and prosecute cryptocurrency cases, but it will develop strategic priorities for future DOJ actions and partnerships.*

In October 2021, the DOJ took a major step to address concerns about cryptocurrency's susceptibility to abuse. On Oct. 6, 2021, Deputy Attorney General Lisa Monaco announced the creation of the National Cryptocurrency Enforcement Team (NCET) to spearhead complex investigations and prosecutions of criminal misuses of cryptocurrency and to recover the illicit proceeds of crimes facilitated by cryptocurrency.

The new team will combine the know-how from various units within DOJ's criminal division with the most relevant experience, namely, the Money Laundering and Asset Recovery Section and the Computer Crime and Intellectual Property Section (CCIPS), along with prosecutors from U.S. Attorney offices across the country who have developed cryptocurrency-related expertise.

The expectation is that bringing together these focused talents will enable the NCET to address the most complex cryptocurrency crimes committed by virtual currency exchanges, as well as crimes committed by "mixing" and "tumbling" services, which charge customers a fee to send cryptocurrencies to a designated address in a manner designed to conceal the currency's source. As described below, the DOJ is not new to cryptocurrency-related prosecutions, but it is now geared up for bigger battles ahead that will require more seasoned hands.

The announcement of the NCET's creation likely did not come as a surprise to those who have been following the DOJ's public statements and actions in the cryptocurrency arena. The Department's attention to the issue began to take shape in February 2018, when then-Attorney General Jeff Sessions established the Cyber-Digital Task Force. The Task Force's mission was to evaluate the impact of recent tech advances, including cryptocurrency, on law enforcement's ability to keep people safe.

By July 2018, the Task Force issued its first report on cyber-enabled threats. The report recommended that the "Department should continue evaluating the emerging threats posed by rapidly developing cryptocurrencies that malicious cyber actors often use."

In October 2020, the Task Force issued the Cryptocurrency Enforcement Framework (the Framework). The Framework describes DOJ's view that cryptocurrency, for better and worse, is likely here to stay and needs to be addressed by law enforcement. In doing so, the DOJ acknowledges the transformative power of cryptocurrency and blockchain technology, as well as cryptocurrency's ripeness for abuse.

*For companies in the cryptocurrency space, be prepared for increased scrutiny by the DOJ and its partner regulatory agencies.*

The Framework details three broad categories of illicit cryptocurrency use: first, to engage in financial transactions to facilitate the commission of crimes, such as drug trafficking or supporting terrorists; second, to hide illegal financial activities through, amongst other things, money laundering, sanctions and tax evasion; and third, to commit crimes in the crypto market itself, through market manipulation, the promotion of scams, and stealing from cryptocurrency exchanges.

The Framework also details the law enforcement structure already in place to address criminal actors utilizing cryptocurrency for malicious ends. This includes myriad federal criminal statutes that prosecutors have been and will continue to use to charge crypto-criminals.

The Framework further emphasizes the value of DOJ partnerships with a number of federal agencies, including the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), the Office of Foreign Assets Control (OFAC), and the Internal Revenue Service (IRS) for achieving its mission.

Some of these agencies, such as the SEC and the CFTC, have been pursuing cryptocurrency-related frauds and scams for years, including in parallel actions with the DOJ.

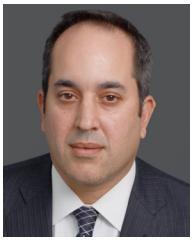
By institutionalizing the Framework's core ideas into a discrete body within the DOJ, the NCET will strengthen the DOJ's capacity to "dismantle the financial entities that enable criminal actors to flourish ... from abusing cryptocurrency platforms," Deputy Attorney General Monaco said in a statement announcing the NCET's creation.

The NCET will not only investigate and prosecute cryptocurrency cases, but it will develop strategic priorities for future DOJ actions and partnerships. The NCET will also, amongst other things, coordinate with federal, state, local, and foreign law enforcement agencies to prepare the government at all levels — as well as our foreign government partners — to meet the challenges posed by this new technology.

The expectation is that the NCET will provide the DOJ with a means for addressing more sophisticated crimes committed in connection with cryptocurrency exchanges. Many of the DOJ's prosecutions to date of exchanges have been relatively low-hanging-fruit frauds. For example, the DOJ has prosecuted individuals responsible for Ponzi and "pump and dump" schemes that have sought to take advantage of retail investors' fear of missing out on cryptocurrency gains, a growing concern of the DOJ.

For companies in the cryptocurrency space, be prepared for increased scrutiny by the DOJ and its partner regulatory agencies. Until further regulation in the space, regulation through enforcement will have to suffice. As such, companies would be well-advised to assess their compliance programs for suitability to address cryptocurrency-related risks. This goes for domestic companies as well as overseas companies doing business in the U.S. or with U.S.-based customers. The DOJ takes a broad view of its jurisdiction, so do not be complacent when it comes to avoiding the long arm of the law.

## About the authors



**Daniel L. Stein** (L) is a partner in **Mayer Brown**'s New York office. He leads the firm's global Regulatory & Investigations group and is a co-leader of the White Collar Defense & Compliance group. A former federal prosecutor, he has extensive experience in regulatory enforcement, government and internal investigations, white-collar criminal defense and complex civil litigation. He counsels clients in a range of complex issues, including U.S. Department of Justice, Securities and Exchange Commission, and Financial Industry Regulatory Authority investigations and enforcement actions. He can be reached at dstein@mayerbrown.com. **Glen A. Kopp** (C) is a partner in the New York office and a member of the Litigation & Dispute Resolution and White Collar Defense & Compliance practices. He is a former Assistant U.S. Attorney in the Southern District of New York and focuses on a number of areas for clients, including commodities and securities fraud, corporate compliance, insider trading, Foreign Corrupt Practices Act internal investigations, and criminal antitrust. He counsels clients facing scrutiny by enforcement and regulatory authorities, including the U.S. Department of Justice, the Securities and Exchange Commission, and state enforcement agencies. He can be reached at gkopp@mayerbrown.com. **Brendan J. Harrington** (R) is an associate in the New York office of the firm and a member of the Litigation & Dispute Resolution group. He can be reached at: bjharrington@mayerbrown.com.

**This article was first published on Reuters Legal News and Westlaw Today on November 30, 2021.**