coinbase

Testimony of John Kothanek

Before the U.S. House Committee on Homeland Security,
Subcommittee on Intelligence and Counterterrorism
Thursday, Jun 9, 2022
9:00 am ET

Chairwoman Slotkin, Ranking Member Pfluger, and Members of the Subcommittee, thank you for this opportunity to testify on the role of crypto in combating terrorism and criminal activity.

My name is John Kothanek and I serve as the Vice President for Global Intelligence at Coinbase. I am responsible for standing up, training, and managing our teams around the world in investigating and combating crypto-related criminal activity on our platform and across the Internet. We work with all levels of United States and foreign law enforcement on large scale cybercrime and criminal investigations, providing best-in-class service, training, and investigative support.

I came to Coinbase in 2014 after meeting with our CEO Brian Armstrong and co-founder Fred Ersham to discuss their vision for the company and the future of crypto. They were laser focused on becoming the most secure, trusted, and compliant onramp for buying, selling, and trading crypto. That has always meant keeping bad actors off the platform. They knew they wanted to build a team that was part of the solution, not part of the problem. That's why I joined Coinbase, and how I've built the Global Intelligence team. Our mission is to protect our customers, crypto, and the country. As a former Marine and son of an Air Force pilot, I have spent most of my life thinking about how to stop bad actors from hurting Americans. I took my experience from the military to the private sector, when I joined Paypal's then-new anti-fraud team in 2000. My goal was to use new technological tools to find illicit transactions and distinguish them from legitimate ones. We built a program from the ground up that became the industry standard. We've done the same at Coinbase.

Our Global Intelligence team is one piece of the puzzle at Coinbase. Our company is a leading provider of end-to-end financial infrastructure and technology for the cryptoeconomy. We define the cryptoeconomy as a fair, accessible, efficient, and transparent financial system for the internet age that leverages digital assets built on blockchain technology. Coinbase Global, Inc. (COIN) became a public company registered with the SEC and listed on Nasdaq in May 2021. Our primary operating company, Coinbase, Inc., and our affiliates (collectively, "Coinbase") make up one of the largest digital asset financial infrastructure platforms in the world, including our exchange for digital assets.

Our global platform enables millions of individuals, businesses, and developers in over 100 countries to participate in the cryptoeconomy. More than 89 million individuals rely on Coinbase to provide a safe, trusted, and easy-to-use crypto account to buy, sell, store, spend, earn, and use crypto assets. We also offer a comprehensive solution that combines advanced trading, custody services, and financing for roughly 11,000 institutional customers. On top of our retail and institutional services, we provide technology and services, such as Coinbase Cloud, that enable more than 185,000 developers to build crypto-based applications and securely accept crypto assets as payment.

Coinbase is the largest U.S. digital asset exchange. We currently list 172 assets for trading and 212 assets for custody on our platform. Every asset listed on the Coinbase platform is subject to a rigorous legal, compliance, and security review. With an early focus on regulatory requirements, Coinbase has strived to set the standard for legal and regulatory compliance in

the digital asset industry. We are licensed as a money transmitter in 42 states, hold a "BitLicense" and a New York Trust Charter from the New York Department of Financial Services, and are authorized to engage in consumer lending in 15 states.

More specific to the interests of this Subcommittee, we are federally registered as a money services business with FinCEN and we serve on the Department of the Treasury's Bank Secrecy Act Advisory Group. Additionally, our activities are subject to federal oversight from the Internal Revenue Service, the Commodity Futures Trading Commission, the Securities and Exchange Commission, the Federal Trade Commission, and the Consumer Financial Protection Bureau.

Coinbase has worked to develop best-in-class criminal investigative methods. We have trained state, federal, and international law enforcement agencies to identify and pursue illicit use of digital asset technologies, and we host law enforcement for in-house secondments to partner with my team on blockchain investigations. We have twice been recognized by FinCEN for providing essential intelligence to law enforcement authorities. In 2019, we received the Private/Public Partnership award from Homeland Security Investigations for our contribution to major law enforcement investigations.

Since Day 1, we have gone after the bad guys. We take a comprehensive approach to combating illegal activities, looking across not only the blockchain but the internet in general. Before we explore how we combat terrorism and other illicit activity, it is important to level set on a few key terms.

Blockchain technology is enabled by cryptography. At the core of all cryptocurrencies or digital assets are private keys – complex and secret numbers used by an individual transacting on the blockchain. A private key is mathematically linked to a public key, which is the address that others can use to transact with the owner of the private key. Put simply, a distributed ledger – a blockchain – is really just the history of transactions between public keys. A transaction occurs if the private key associated with the public key cryptographically signs off on the transaction.

Blockchain technology creates a ledger of transactions that are transparent and immutable. However, unlike traditional ledgers, there is no need for a central authority to maintain the database. Blockchain-based ledgers are public, distributed, and immutable: anyone can download the ledger and see the entire history of every transaction that has ever occurred on a given blockchain and nobody can change it. That free public history is an essential feature of a blockchain because it ensures visibility into the counterparties involved in the transaction. It also enables more robust criminal investigations.

This is contrary to many of the narratives surrounding crypto, but the reality is that blockchain technology can help identify and prevent criminal activities. Cryptocurrency is easier to track than fiat currency because searchable databases (public blockchains) exist for most transactions. The information in these blockchains exists permanently, and provides law enforcement with details about crypto transactions that are not available with fiat currency. The

Department of Justice discusses this utility as part of its investigation methods; the September 2019 edition of the *Department of Justice Journal of Federal Law and Practice* says:

> *Cryptocurrency, despite the purported anonymity it grants criminals, provides law enforcement with an exceptional tracing tool: the blockchain. While the blockchain's historical ledger will not list the names of parties to transactions, it provides investigators with ample information about how, when, and how much cryptocurrency is being transferred.*[1]

The public blockchains have helped advance law enforcement efforts with new tools that reveal the structure of organized ransomware crime rings and individual hackers in ways that are unavailable with fiat.

I would now like to describe in more detail Coinbase's efforts to fight crime and protect our customers. From the very early days of the company, we have been committed to preventing criminals from abusing our platform and our customers. We feel a strong obligation to protect our customers, our company, and the crypto ecosystem as a whole from bad actors. If this technology is going to succeed, ordinary people need to be able to trust and safely interact with the crypto-economy.

We attack illicit activity on our platform from a variety of angles. As one of the first regulated digital asset exchanges in the United States, we quickly developed robust Anti-Money Laundering (AML) and Know Your Customer (KYC) programs. Our Financial Crimes Compliance team uses a proprietary transaction monitoring system to identify potentially illegal activity so that we can file Suspicious Activity Reports with FinCEN and, if necessary, close those accounts.

Our Financial Crimes Compliance program incorporates all of the traditional components and controls you would expect from a financial institution, and it is further bolstered by a characteristic unique to cryptocurrency – the public ledger of transactions within the blockchain. By reviewing publicly available blockchain data, especially with the aid of sophisticated blockchain analysis tools like Coinbase Tracer, both our compliance and global investigations teams are able to trace the proceeds of crime and attribute blockchain addresses to known entities, including criminal entities. Once we confirm that an address is associated with crime – for example, an address used to receive stolen funds or an alleged terrorism financing address – we are able to block other customers from sending to that address and trigger automatic alerts for any customers attempting to do so.

Another key component of our strategy to combat crime is our relationship with law enforcement. We have been committed since the beginning to building a collaborative partnership with law enforcement. In fact, my department, the Global Intelligence team, was created in 2016 to focus almost exclusively on law enforcement investigations and outreach

[1] 67 DOJ J. FED. L. & PRAC., No. 3 at 166 (2019).

efforts. Our mission in this respect is simple: do everything we can, within the bounds of our strict privacy commitments to our customers, to help law enforcement pursue bad actors in the crypto space.

We do this in several ways. First, as I mentioned earlier, we have offered cryptocurrency investigations training, free of charge, to thousands of law enforcement officers around the world. These trainings range from short sessions on the basics of cryptocurrency to day-long intensive workshops. Our philosophy is that the better law enforcement understands cryptocurrency and the ways in which public blockchains can be analyzed to detect and investigate criminal activity, the more effectively they can safeguard our customers and the ecosystem as a whole.

Our investigators spend hours with law enforcement each week explaining how to interpret the blockchain information in our subpoena responses and directing officers to the tools and resources they need to pursue their investigations. If we see an opportunity to help a law enforcement officer who does not have access to blockchain analysis tools, perhaps by helping them trace ransomware payments or stolen funds, we do it without hesitation.

We have also had the honor of being invited to speak at numerous law enforcement conferences and we have frequently been asked to brief senior law enforcement officials on cryptocurrency trends. For example, we recently worked with the REACT Task Force, also know as the Regional Enforcement Allied Computer Team Task Force, in San Jose on a joint briefing for the Secretary of Homeland Security on the topic of crypto account takeovers and investment scams. We have also briefed senior leadership within the Secret Service, and we recently hosted a Secret Service agent for a three-month secondment with my team.

The teaching and sharing go both ways. Some of the world's leading crypto investigations experts work for U.S. law enforcement agencies, and we are fortunate to be learning from them on a daily basis. We frequently participate in various public-private sector working groups and meet with law enforcement partners to learn about trends in crypto-related crime that may be affecting our customers. We, in turn, can use this information to enhance our compliance programs.

An example of this is the quarterly investigative "sprints" that my department organizes, each focused on a specific crime type, where we solicit large amounts of data and blockchain intelligence from law enforcement partners around the world and conduct in-depth investigations. Our two most recent sprints focused on Child Sexual Abuse Material ("CSAM") and ransomware, and both resulted in actionable intelligence to law enforcement. This would not be possible without the close relationships we have built with law enforcement.

While we are proud of our successes investigating criminal activity, there are several major challenges we face. A small group of non-compliant foreign crypto exchanges are the venues used by criminal actors to cash out their illicit gains, and those foreign exchanges use jurisdictional arbitrage to avoid U.S. regulations. The industry as a whole is seeing crypto stolen

through scams and thefts going to bad actors overseas, usually via unregulated exchanges. Criminal actors generally avoid exchanges, like Coinbase, that have AML/KYC programs because they would likely be identified by us, have their account frozen, or referred to law enforcement. As an example, research indicates that from 2017-2019, over 80% of ransomware cashout activity was handled by just four offshore entities.[2] 2021 data so far shows that ~64% of ransomware cashouts occurred on just three foreign exchanges. Of the top 10 recipients of ransomware payments, eight are offshore exchanges and two are mixing services.

Further, despite the incredible proliferation of crypto investigation expertise throughout law enforcement agencies over the last several years, we often run into situations where law enforcement – especially at the local level – lacks the tools and resources necessary to pursue crypto-related crime. This is especially true in large-scale cases where victims may be located across the country, or in cases where the criminals are based overseas.

The U.S. Government should develop tailored solutions in this space to effectively target illicit activity that uses crypto. We know that a vast amount of illicit activity is happening on a small set of non-compliant offshore exchanges and mixing services that enable criminal actors to monetize their activity. While the Department of Justice has authority to prosecute individuals and entities involved in facilitating illicit activity, even when that activity is located abroad, directing more of law enforcement's investigations and resources to pursue those bad actors could very effectively disrupt those actors' infrastructure in the near-term. Further, we would recommend that Congress ensures law enforcement is well equipped to develop local-state-federal task forces to share information and combat illegal activity, as well as fund international partnerships that will help combat efforts by unregulated international entities to move crypto in a manner that facilitates illegal activity.

In closing, thank you Chairwoman Slotkin, Ranking Member Pfluger, and Members of the Subcommittee for holding this important hearing today. Coinbase is committed to working with Congress and law enforcement to combat illicit finance and terrorism, while also protecting the privacy and security of our customers. Combating illegal activity on our platform is core to our mission of enabling economic freedom in a trusted, secure, and compliant way. Thank you and I look forward to answering your questions.

[2] Chainalysis 2021 Crypto Crime Report (Jan. 19, 2021).