coinbase

Testimony of Grant Rabenn
Director, Financial Crimes Legal

Before the U.S. House Committee on Financial Services
Subcommittee on Digital Assets, Financial Technology, and Inclusion

Thursday, February 15, 2024

coinbase

Chairman Hill, Ranking Member Lynch, and Members of the Subcommittee, thank you for this opportunity to testify on the important role of crypto in combating terrorism and criminal activity.

My name is Grant Rabenn and I serve as the Director of Financial Crimes Legal at Coinbase. I lead a team that acts as internal legal counsel to our compliance, global investigations, and product teams on anti-money laundering, sanctions, and law enforcement matters. We work collaboratively with all levels of global law enforcement to keep our platform, and the digital asset ecosystem, safe.

I have spent most of my professional life prosecuting financial crimes, going after bad actors, and preventing them from using technology to hurt Americans. I joined Coinbase in 2021, after a decade of public service as a federal prosecutor, to continue that work at a critical time in the development and growth of crypto technology. I began my career in public service at the Department of Justice, running a money laundering task force that used suspicious activity reports to generate a wide variety of cases, ranging from public corruption to drug trafficking to child exploitation. I initiated some of the federal government's earliest criminal investigations into crypto-related money laundering, including FinCEN's first enforcement action against an unlicensed peer-to-peer crypto exchange. I also played a leadership role in the takedown of the world's largest darkweb marketplace, AlphaBay, which was described as the most successful cybercrime prosecution in the history of the internet, and for which I was awarded the Attorney General's Award, the FBI Director's Award, and the Director of National Intelligence's Meritorious Service Award.

I also formed one of the DOJ's most successful darkweb and cryptocurrency money laundering task forces, NCIDE (the Northern California Illicit Digital Economy Task Force) in conjunction with the FBI, Homeland Security, and IRS Criminal Investigations. Leveraging this task force, I prosecuted dozens of darkweb drug traffickers, crypto money launderers, and other cyber criminals, including the prosecution and takedown of Wall Street Market, another global, large darkweb marketplace. I also worked with Main Justice to train investigators and prosecutors around the country and internationally on the ins and outs of crypto money laundering and darkweb investigations. In my latter years at DOJ, I also held a leadership position in the FBI's Northern California Cybercrime Task Force, in which we investigated ransomware, malware-as-a-service, and nation state hacking, and served as my district's cyber fraud coordinator.

I left the government after a decade of hard work to apply my skills and experience at Coinbase because I believe in the critical role of the private sector in combating illegal activity. Coinbase is the largest U.S. digital asset exchange, and has been a public company since April 2021. We serve millions of retail and institutional customers on our platform, and are providing technology services and building new tools for blockchain developers around the world.

Senior leaders at Coinbase were then – and remain – laser focused on being the most secure, trusted, and compliant platform for buying, selling, and trading crypto. That has always meant keeping bad actors off the platform. They wanted to build a team that was part of the solution,

and that's how I've built the Financial Crimes Legal group. Our mission is to protect our customers, crypto, and the country. Just like me, hundreds of former national security and compliance professionals have joined the fight for the security of crypto in America. Together we have built a program that has become the American-made, industry gold standard.

I am pleased to speak with you today about Coinbase, our hand-in-glove partnerships with law enforcement, our work to stop bad actors attempting to use our platform, and our views on the legal environment for financial crimes and crypto. Although the U.S. Treasury Department noted in its *National Money Laundering Risk Assessment* just last week that "the use of virtual assets for money laundering remains far below that of fiat currency and more conventional methods that do not involve virtual assets,"[1] this is still a critical issue. Criminals use many methods to launder money and finance illicit activity, ranging from dealing in cars to gold bars to real estate to cash. But we are committed to making sure crypto is part of the solution, not the problem.

There are four main points I would like to share with you today in my testimony. At a high level:

- Embracing and leading in blockchain and crypto technology is crucial for the U.S. to maintain its global leadership and protect national security, as these areas represent modern battlefields for technological supremacy. Keeping the crypto industry within U.S. jurisdiction ensures compliance with laws, enhances law enforcement capabilities, and secures the financial system against external threats and vulnerabilities.
- Coinbase has invested heavily to build a world-class, industry-leading Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) program. We have worked with regulators for more than a decade to establish a program that leverages new technology and rivals that of any traditional finance institution. The crypto industry takes seriously its obligation to protect Americans, and the U.S. should take seriously its obligation to help this innovation grow responsibly in America.
- Sanctions evasion, terrorist finance, and criminal activity is highly concentrated on a few noncompliant offshore exchanges. Law enforcement should more fully utilize the extensive legal tools at its disposal to police those exchanges today. There is, in other words, an enforcement gap that needs to be addressed much more so than a regulatory gap. If additional funding is needed so law enforcement has the resources to prioritize crypto investigations, Congress should provide it immediately.
- Coinbase is supportive of legislation providing additional tools that will make crypto a safer place. Legislation should ensure that new powers don't impede existing law enforcement tools that currently enable crime-fighting partnerships, are appropriately targeted, and do not have unintended consequences of impeding development of a robust crypto economy in the United States.

[1] See United States Department of Treasury, 2024 National Money Laundering Risk Assessment (Feb. 2024), at 59, available at https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf.

The National Security Imperative

The future of the country's global leadership depends on its willingness to embrace its leadership in technology. Right now, the U.S. faces unprecedented threats to this leadership position, and one of the key battlefields is crypto and blockchain. There is a national security imperative to embrace these technologies consistent with the interests of the United States, its citizens and our country's tradition of innovation. There is no doubt that this is possible. History proves that when the U.S. commits to leading in a particular area, it has always succeeded.

The U.S. government has much to gain by keeping the crypto industry onshore: regulators can ensure compliance with AML regulations; law enforcement can directly subpoena records from U.S. companies (as opposed to having to use cumbersome, treaty-based methods to get records from overseas); and consumers can use Virtual Asset Service Providers (VASPs) subject to the broad array of domestic regulatory protections. The reverse is true: if the pipes and plumbing of a technology that moves value flow elsewhere, the U.S. government loses its ability to shape it.

The benefits of leveraging crypto and blockchain technology are real, but the technology itself is complex. Before going further, I would like to level-set on some key terms and technological concepts. Blockchain technology is rooted in 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, immutable, and available to any law enforcement or investigation team. Unlike traditional ledgers, there is no need for a central authority to maintain the database or give access approval. Blockchain-based ledgers are public, distributed, and permanent: 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 means that crypto companies, regulators, and law enforcement can analyze transactions carried out on that blockchain whether or not they took place on the company's own platform. In contrast, a traditional financial institution is largely limited to using private, opaque ledgers that are only available to that specific institution. This creates significant risk of blind spots for traditional financial institutions because it is difficult—if not impossible—for them to fully monitor transactions that happen off of their individual platforms. For example, if a bank's client wants to deposit funds into an account, the bank must rely on information provided by the customer about the source of those funds, or manually reach out to other financial institutions to share

information pursuant to FinCEN rules, instead of being able to independently and immediately analyze the full history of those funds. Crypto fixes this problem by giving unprecedented access to the full scope of transactional records. This is often referred to as "know your transaction," (KYT) which is an entirely new sphere of compliance information unavailable in traditional finance.

It runs contrary to many of the narratives surrounding crypto, but the reality is that blockchain technology can help identify and prevent criminal activities. Both the government and journalists have recognized the huge compliance and investigatory advantage provided by crypto. As the DOJ noted in its legal practice journal in 2019:

> *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.*[2]

Public blockchains have helped advance law enforcement efforts with new tools that reveal the structure of terrorist groups, "deanonymize" illicit actors, and go after organized ransomware crime rings and individual hackers in ways that are unavailable with fiat. This additional data lets us conduct sophisticated analyses to determine the risk of a specific transaction or asset (KYT), instead of relying solely on Know-Your-Customer (KYC) information and transactions happening within our platform.

KYT is groundbreaking for compliance because it is generally *immediate* (the information is available on the blockchain), *independent* (it does not have to come from the customer and cannot be tampered with),[3] and *dynamic* (the risk associated with a customer or transaction can be continually reevaluated based on new blockchain data). Companies like ours can then combine KYT with traditional compliance tools to enhance their risk ratings of customers associated with those transactions. If the rating rises to a certain level, platforms can take further action, such as conducting enhanced diligence reviews, filing a Suspicious Activity Report (SAR), or closing the account.

KYT also creates an enhanced approach to sanctions compliance in which companies like Coinbase directly screen for crypto addresses identified by the Office of Foreign Assets Control (OFAC) and can then proactively build out larger networks of high-risk addresses. Before the advent of crypto, OFAC was limited to putting static, traditional identifiers—such as names and

---

[2] 67 DOJ J. FED. L. & PRAC., No. 3 at 166 (2019).

[3] *See* Robert Werner, et al., *Blockchain Analysis Tool of Cryptocurrency*, ICBCT '20: Proceedings of the 2020 The 2nd International Conference on Blockchain Technology 80 (Mar. 2020), https://dl.acm.org/doi/pdf/10.1145/3390566.3391671 ("The blockchain … is an immutable ledger, which is stored on a large network of servers worldwide in a decentralized manner. On this ledger, all transactions are stored permanently, transparently and can be accessed by anyone.").

addresses—on its Specially Designated Nationals (SDN) List. But with blockchain technology, sanctions compliance can now be based on transactional data, not just personal identifying information (PII). With blockchain analytics, platforms can take ground-truth addresses provided by OFAC to build out and identify much larger networks of high-risk counterparties using blockchain heuristics. From a relatively small number of blockchain addresses identified by OFAC, platforms can build out large networks of addresses that they do not allow customers to transact with. They can do this by leveraging immutable transactional data on the blockchain that is unrestricted by private ledgers and can tell them about common ownership.

Coinbase's Commitment to Fighting Financial Crime

Coinbase was founded with the goal of being the world's most trusted, compliant, and safe crypto platform. With this early commitment to customers and safety, Coinbase has strived to set the standard for legal and regulatory compliance in the digital asset industry. Coinbase is currently regulated by more than 50 regulators in the U.S. alone: we are a money services business registered with the US Treasury Department and subject to Financial Crimes Enforcement Network (FinCEN) rules, and we have served on the Department of the Treasury's Bank Secrecy Act (BSA) Advisory Group. We have 45 state money transmission licenses, and a BitLicense and state trust charter from the New York Department of Financial Services (NYDFS). We are a licensed designated contract market (DCM) and a futures commission merchant (FCM) regulated by the CFTC, and Coinbase Asset Management is a registered investment advisor under the SEC. Internationally, we are also subject to regulatory supervision in a number of markets, including the United Kingdom, European Union, and Singapore; these regulators also have a heavy focus on financial crimes and mandate implementation of strong AML programs.

Coinbase has implemented robust legal and investigations programs to protect our customers, our company, and the crypto ecosystem from bad actors. We believe that if this technology is going to succeed, ordinary people must be able to trust and safely interact with the crypto-economy. We've built a global AML program based on best practices from our team members' cumulative decades of experience in the traditional financial services space. This is hard work, and we've learned throughout this process how to build a compliance program which continuously strives to meet our regulators' and our own high expectations. We now employ more than 400 compliance, legal, and investigation professionals, including former public servants with decades of experience with major law enforcement agencies such as DOJ, FBI, OFAC, FinCEN, and Scotland Yard, as well as some of the biggest names in traditional finance.

As described below, we apply KYC to our customers when onboarding them, monitor and review transactions for suspicious activity, file SARs, and regularly and proactively engage with law enforcement, even when we are not required to do so. 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 us on blockchain investigations. We have received the FinCEN Director's Law Enforcement Award three times, in recognition of

Coinbase's provision of essential intelligence to law enforcement authorities through Suspicious Activity Reports. In 2019, we received the Private/Public Partnership award from Homeland Security Investigations for our contribution to major law enforcement investigations.

Coinbase's Crime Fighting Tools in Practice

We attack illicit activity on our platform through a multi-layered, robust, and comprehensive compliance program, and from a variety of angles. Our Financial Crimes Compliance team uses a proprietary transaction monitoring system to identify potentially illegal activity so that we can file SARs with FinCEN and, if necessary, report directly to law enforcement, and close those accounts. We also incorporate all of the traditional components and controls you would expect from a major financial institution. This work begins in the customer onboarding process. Whenever someone wants to open an account on Coinbase.com, we KYC them. The information we request may include, but is not limited to, personal information such as the customer's name, residential address, telephone number, email address, date of birth, taxpayer identification number, government identification number, their banking information, mobile device identifiers (*e.g.*, international mobile subscriber identity and international mobile equipment identity) and other details. The product of that work generates a risk score for that customer. Based on that score, they may also be required to undergo "Enhanced Due Diligence" (EDD), where Coinbase may request additional information, including information of the customer's source of funds, wealth and expected activity to determine if this is a customer we want to put on our platform. The customer risk score is dynamic; a customer that was not subject to EDD during onboarding may be subject to it later on based on their platform activity.

Our work is further bolstered by a characteristic unique to crypto: 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, our proprietary in-house technology, 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 (*e.g.*, 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. When an alert is triggered, we can then carry out additional diligence on the customer, investigate for potential SAR filing, or take other measures.

To put this in perspective: OFAC has only listed roughly 560 crypto addresses in total, most of which are associated with bad offshore actors who are not compliant or beholden to U.S. law. Through our proactive research and analytics, Coinbase has identified transactions associated with those addresses (*e.g.,* "clustered") and then blocked users from transacting with them. Through this clustering, Coinbase has an expanded aperture for sanctioned parties and other illicit actors, which now covers over *8 million* related crypto addresses, including those tied to terrorism financing and other forms of illicit finance. Traditional name screening methods simply do not have this reach.

Whenever we can, we stop funds from flowing to bad actors in real time. Coinbase has developed an innovative sanctions Interdiction Solution to conduct real-time screening of incoming and outgoing crypto transactions. Coinbase blocks funds coming from, or going to, a sanctioned cryptocurrency address, either because the address was identified specifically by OFAC or added to the transaction blocklist as a result of Coinbase's proactive investigations. If a transaction is sent to or received from an address that is considered sanctioned, those funds will be intercepted, sent to an internal, segregated wallet, and a blocked property report will be filed with OFAC.

The technology behind our Interdiction Solution also allows Coinbase to immediately respond to major illicit finance events like FinCEN's designation of dirty crypto exchange Bizlato, and the many rounds of new sanctioned addresses tied to Russia's invasion of Ukraine. We can do this because our systems are calibrated for automatic feeds from OFAC's SDN List, we have professionals that stay on top of government actions like Special Measures, and our tools like Coinbase Tracer can engage in rapid analysis and clustering of potentially affiliated addresses. Moreover, our dedicated sanctions team – led by personnel who joined Coinbase directly from OFAC – has robust protocols to help ensure all changes are identified and implemented as required.

Another key component of our strategy to combat crime is our proactive and dedicated relationship with law enforcement. Coinbase works regularly with global law enforcement agencies to help combat terrorism financing, sanctions violations, ransomware, drug trafficking (including fentanyl production), money laundering, and darknet activity, such as identity theft, sale of hacking tools, and child exploitation. We have been committed since the beginning to building a collaborative partnership with law enforcement. 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, under existing legal requirements, we must be responsive to law enforcement requests for information, including Section 314(a) information requests, and may voluntarily participate in information sharing with other financial institutions via 314(b). We are required to maintain monitoring systems to identify potentially suspicious activity and file Suspicious Activity Reports with FinCEN. If we believe an account is associated with a bad actor, we have an obligation to review it, and if necessary, report it to law enforcement and close it down.

We go above and beyond what is required by the law, however. As I mentioned earlier, we have offered crypto investigations training, free of charge, to thousands of law enforcement officers around the world. These trainings range from short sessions on the basics of crypto to intensive workshops. Our philosophy is that the better law enforcement understands crypto 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.

Law enforcement agencies domestically and internationally actively rely on Coinbase's intelligence and training to understand and combat illicit activity. We have trained U.S. intelligence and law enforcement officials at the highest levels, had the honor of being invited to provide critical insight at global law enforcement training, and we are frequently asked to brief senior law enforcement officials on crypto trends.

Just this week, Coinbase personnel are meeting with the instructors at the Federal Law Enforcement Training Center on new training programs. We work almost daily with the REACT Task Force, also known as the Regional Enforcement Allied Computer Team Task Force, currently co-leading a task force on "pig butchering" scams. We are also working with the Secret Service on similar issues, and last year we hosted a Secret Service agent for a three-month secondment with our Global Intelligence team. We also recently joined a briefing for the Secretary of Homeland Security on the topic of crypto account takeovers and investment scams. Our desire is always to share what we know to protect the country.

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, use this information to enhance our compliance programs.

The Global Legal Environment for AML and Compliance in Crypto

While we are proud of our successes investigating criminal activity, there are several major challenges we face. Crypto stolen through scams and thefts is generally going to bad actors overseas. Today U.S. law enforcement and regulators have broad AML authorities. Any business or entity serving U.S. persons or doing business in the United States that takes custody of customer assets is required to implement effective AML programs,[4] including KYC, transaction monitoring, SARs, appointing a BSA officer, and training employees on compliance

[4] *See, e.g.*, 31 CFR § 1022.210(a) (requiring money services businesses to have "[a]n effective anti-money laundering program … that is reasonably designed to prevent the money services business from being used to facilitate money laundering and the financing of terrorist activities.").

requirements. The businesses do not need to be physically located in the United States,[5] as recent high profile enforcement efforts have demonstrated.

Yet a small group of non-compliant foreign exchanges continue to serve as the venues used by criminal actors to cash out illicit gains earned both in the U.S. and abroad. Criminal actors generally avoid American exchanges, because they are required to implement AML/KYC programs, and they work closely with law enforcement to freeze assets and investigate further.[6] Instead, criminals flock to exchanges which fail to implement these controls to reduce their likelihood of detection. In turn, those exchanges take advantage of gaps in global enforcement efforts by engaging in jurisdictional arbitrage, providing crypto services to global customers while having weak (or non-existent) AML controls, with the expectation that regulators will not hold them accountable.

This problem is especially acute when it comes to the "on-ramp" and "off-ramp" to fiat. By design, the crypto universe is a closed system – even a stablecoin, a digital representation of a dollar, is not an actual dollar. In general, fiat must first be converted into crypto tokens in order to engage with the digital asset ecosystem. Likewise, those tokens must be converted back to fiat in order to cash out.

This makes the on- and off-ramp the most critical part of the ecosystem from an AML point of view. As noted above, in the U.S., exchanges must comply with AML procedures. That is not true in every country across the world. And traditional banks in some countries are doing business with non-compliant exchanges, providing a means for bad actors to cash out.

One of the most effective ways to combat illicit finance, therefore, is to disrupt the ability of noncompliant VASPs to liquidate and conceal criminal proceeds, which makes criminal behavior less profitable. As noted below, **we strongly support FinCEN and law enforcement getting additional resources directed at making enforcement of AML rules on noncompliant exchanges a priority, which would likely have an immediate effect.** For banks that are aiding in sanctions evasion as an on- or off-ramp, traditional sanctions authority could be applied.

---

[5] *See* 31 C.F.R. § 1010.100(ff); *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001, at 12 (May 9, 2019) ("FinCEN 2019 Guidance") (emphasizing that the BSA's "requirements apply equally to domestic and foreign-located [crypto] money transmitters doing business in whole or in substantial part within the United States, even if the foreign-located entity has no physical presence in the United States.").

[6] U.S. Dep't of Justice, *The Report of the Attorney General Pursuant to Section 5(b)(iii) of Executive Order 14607: The Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related Digital Assets* 7 (Sept. 6, 2022), https://www.justice.gov/ag/page/file/1535236/download ("DOJ Digital Assets Report") (cautioning that "criminals continue to take advantage of noncompliant actors … including noncompliant cryptocurrency exchanges … to exchange their cryptocurrency for cash or other digital assets without facing rigorous [AML] scrutiny.").

Legislative Solutions

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 offshore exchanges that attract and enable criminal actors to monetize their activity because they are not obligated to comply with U.S. law. 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. To the extent that additional authorities might enhance that work, we support them so long as they do not prevent the lawful use of crypto, or make the regulatory environment uninhabitable such that the technology goes overseas. Below are items we think are especially important to consider.

Clarify Legal Powers to Reach Offshore Exchanges

As noted above, bad actors generally avoid exchanges that have real AML/KYC programs because they would likely be identified, have their accounts frozen, and/or be referred to law enforcement.

The U.S. government should be working to raise the floor in global AML compliance. As Treasury noted in the *National Terrorist Financing Risk Assessment* released last week, "[d]espite the FATF [Financial Action Task Force] extending global standards for AML/CFT to VASPs in 2019, many countries have been slow to regulate VASPs. Many VASPs operating abroad have substantially deficient AML/CFT programs, particularly in jurisdictions where international standards for VASPs are not effectively implemented."[7] According to FATF, countries overall are making slow progress in implementing FATF's guidance for virtual assets; 73 out 98 jurisdictions are only partially or not compliant with the guidance.[8]

Congress can help by clarifying that the most significant legal tools, especially the International Emergency Economic Powers Act (IEEPA), have extraterritorial reach in both crypto and traditional finance. For jurisdictions that are FATF-compliant, local law could substitute from a compliance perspective, which could incentivize countries to raise their own standards.

Additional Enforcement Resources, Focused On Non-Compliant Entities

The U.S. government should use all of its existing tools on non-compliant offshore entities, including partner financial institutions. If a country like North Korea is off-ramping through specific banks, consequences should apply, up to and including sanctions and criminal prosecution.

---

[7] U.S. Dept. of Treasury, 2024 National Terrorist Financing Risk Assessment at 21 (Feb. 2024), available at https://home.treasury.gov/system/files/136/2024-National-Terrorist-Financing-Risk-Assessment.pdf.

[8] Id.

To ensure those investigations are prioritized, law enforcement should be given additional resources and a mandate to focus on crypto, especially through offshore actors. In particular, since the passage of the *Corporate Transparency Act*, FinCEN has had a number of new obligations imposed on it without a comparable increase in budget. Congress should ensure that FinCEN has the resources it needs.

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. 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. Resources from Congress would help close this gap.

Market Structure Legislation

Many policymakers have voiced concerns about the consistent application of AML and sanctions rules across the crypto ecosystem. From our vantage point, the crux of this issue lies in the absence of a uniform federal framework for cryptocurrency regulation in the United States. Pushing the industry beyond US borders does not mitigate risks; rather, it exacerbates them, posing a greater threat to our national security.

In this context, the *Financial Innovation and Technology Act for the 21st Century* (FIT21) stands as a pivotal legislative measure. It creates clear pathways for registration with federal regulators, which come with clear AML/BSA obligations. This bill represents the necessary evolution of our regulatory approach, harmonizing it with the dynamic nature of financial technologies.

Our collective objective should be to incorporate cryptocurrency within our regulatory purview, thereby fortifying our financial systems against illicit activities. The passage of FIT21 is a step in that direction.

Stablecoin Legislation

Likewise, stablecoin legislation is the best way to prevent illicit activity in the stablecoin marketplace. We agree that AML controls are a necessary component of stablecoin construction. As a threshold matter, concerns over illicit finance are a reason to enact a regulatory framework for stablecoins. U.S.-regulated stablecoins with the ability to freeze assets, subject to the protections of American law, are highly disfavored for crime. Drawing more stablecoin issuers onshore will bring with it adherence to regulatory requirements to ensure the government has the most tools available to fight crime and terrorism. Legislation can provide that stablecoins that are not registered in the United States, with appropriate AML controls, cannot be sold to U.S. persons. The *Clarity for Payment Stablecoins Act* accomplishes this, and appropriately so.

Information Sharing

Coinbase participates in information sharing programs whenever it can. Coinbase is a member of FS-ISAC (the Financial Services Information Sharing and Analysis Center) and shares cyber threat intelligence with peer financial institutions to proactively defend against cybercriminals. Coinbase actively participates in the USA PATRIOT Act 314(b) Voluntary Information Sharing program in accordance with FinCEN guidance. We maintain bilateral threat intelligence sharing agreements with other leading blockchain companies. Coinbase also leads industry-driven programs such as the TRUST solution to the Travel Rule. The Travel Rule requires financial institutions to share certain basic information about their customers when sending funds over a certain amount to another financial institution. Coinbase was a founding member of what is now the largest coverage network for crypto, enabling information to be shared between over 75 global VASPs across 15+ different countries with proof of ownership, security and privacy standards, and no central store of personal data.

Crypto-specific information sharing programs, especially in the area of terrorist and illicit finance, would be welcome. Coinbase is currently supporting an industry effort to develop a Crypto ISAC. These programs could be designed to accomplish broader market surveillance objectives which may be desired in connection with market structure legislation.

Cybersecurity

Cyber incidents, hacks, and ransomware do not represent a crypto-specific issue. Like bank robberies and credit card fraud, the cause of the crime isn't the financial instrument. Rather, the causes of the crime are flaws and cracks in security underlying the instrument. In fact, as noted above, crypto makes it easier to track stolen assets than cash, and to follow the flow of funds all over the world. Working with law enforcement, Coinbase has had success recovering funds from unlawful acts, identified bad actors and helped bring them to justice.

Yet, it is undeniably the case that additional cybersecurity measures would make transacting online, including with crypto, more secure. Different companies put different amounts of effort into protecting their customers and assets, in part because of the lack of clear federal crypto regulation. North Korea stole as much as an estimated $1.7 billion in virtual assets through hacks in 2022.[9] The DPRK has targeted the crypto ecosystem: exchanges, blockchain bridge developers, and individuals holding high volumes of digital assets.

The lack of clear standards means that in many cases it isn't malice or fraud that leads to these gaps: it's that the people building these products don't have the expertise to do it at the right level and don't have a guide book to follow. Many of these hacks were not the result of sophisticated hacking techniques but rather flaws in basic security management and protocols. In earlier years North Korea attempted to hack custodial exchanges, including Coinbase, although we successfully detected and defeated those attacks. Much of their recent focus has been on non-custodial crypto services, specifically self-hosted wallets (software allowing

[9] U.S. Dept. of Treasury, 2024 National Proliferation Financing Risk Assessment at 5 (Feb. 2024), *available at* https://home.treasury.gov/system/files/136/2024-National-Proliferation-Financing-Risk-Assessment.pdf.

customers to manage their own funds) and crypto bridges (software services that allows users to transact between different blockchains).

After stealing funds, DPRK will often then take advantage of offshore exchanges and OTC brokers with poor controls in AML, and Chinese banks to cash out. The U.S. government already has tools, including sanctions authority, to go after the financial institutions that are helping North Korea move this money. New regulations on already compliant U.S. exchanges will not prevent North Korea from laundering stolen funds – as the critical AML gap is with those attempting to play jurisdictional arbitrage to evade American regulations.

The best approach to closing the AML gap is for U.S. law enforcement to combine existing tools, and any new ones Congress provides, with a laser focus on holding cyber criminals accountable and putting a stop to this illicit offshore activity. This is an issue that exists across all industries. Crypto hacks are public by nature–any theft of assets is transparent to everyone on the blockchain–but the scourge of cyber crime has an impact on the entire American economy in ways both visible and invisible. We support efforts to strengthen the nation's cyber defenses, including through public-private partnerships, to increase cyber resilience in all sectors of the American economy. Very simply, the nation must up its game. Congress can continue to provide leadership on this critical issue and make this a focal point of the national debate.

Concerning Ideas

Regulation of Blockchain Infrastructure

One highly controversial provision included in the *Digital Asset Anti-Money Laundering Act*, introduced by Senators Warren and Marshall, would make anyone involved in a blockchain transaction, including non-custodial service and software providers such as miners, network validators, and personal wallet providers, a financial institution under the Bank Secrecy Act. That would mean they would be required to collect and retain massive amounts of customer data, file SARs, register with FinCEN, and appoint BSA officers, among other requirements.

Fundamentally, this idea misunderstands how blockchains work. Much like a cloud services provider or a telecommunications company would secure their own networks, miners and validators secure the blockchain network, but they cannot see PII for individual transactions. Nor should we want them to do so. Protecting the privacy of Americans has long been a goal of Congress, but these requirements would put all Americans at huge risk. Blockchain validators are decentralized by design, meaning PII would exist in many, many places. This risk would be further exacerbated by the BSA's requirement to retain data for years.

The bill makes "unhosted wallet providers" Money Services Businesses, but fails to clarify or limit what that means. Read literally, this would impose substantial AML obligations on whomever provides *anything* that could function as an unhosted wallet: not just specially designed hardware but *anything* capable of recording a private wallet key, such as a computer, USB thumb drive – even a paper and pencil.

Congress should oppose these new categories of the BSA.

Regulation of Decentralized Protocols

Adoption of a regulatory framework that captures software infrastructure could lead to challenges. Similar to traditional financial regulation, the role of regulators should be limited to regulation of users of technology, not the technology itself. That means regulation of centralized intermediaries in the crypto ecosystem–whether that is an off-ramp, exchange, or custodian–where AML standards, along with additional transparency and disclosure, are needed. Decentralized services with no intermediary are software code, and should not be regulated like centralized actors.

In particular, policymakers should be careful not to regulate protocols, the set of rules defining how computers communicate with one another. Protocols underlie much of today's internet infrastructure through standards like HTTP (website data exchange), SMTP (email), FTP (file transfer), as well as text messaging protocols SMS and MMS. In crypto, protocols establish how assets are issued, used, transferred, and exchanged. Any user or application can access these protocols. Decentralized finance (DeFi) protocols have been developed on blockchains like Ethereum to enable novel financial applications, and services that connect users. We have only begun to scratch the surface on potential use cases.

As it is autonomous code, a protocol cannot incorporate subjective determinations that traditional AML regulations sometimes require. A protocol cannot interview a customer, or conduct an investigation to determine a source of funds. A protocol cannot appoint a BSA officer. A protocol cannot, on its own, register with FinCEN.

This does not mean that the exchange of value in DeFi should be unregulated. To the contrary, it should be tightly regulated, through the access points that enable the underlying transfer of value. As noted above, the on- and off-ramps are necessary to cash out. Those should be (and in the United States, are) protected at all costs. End users of DeFi protocols should face consequences for illegal activity; just like with cash, if a crime occurs as a result of user action in DeFi, the perpetrators of that crime should face justice.

Conclusion

In closing, thank you Chairman Hill, Ranking Member Lynch, and Members of the Subcommittee for holding this important hearing today. Coinbase knows well these are complicated issues, made harder because 20th century laws weren’t designed for 21st century innovations. Crypto can deliver a more fair, accessible, efficient, and transparent system to transfer value and ownership. If allowed to flourish, the potential enabled by crypto is almost limitless – better access, more equity, cheaper services. Well-designed regulation of digital assets will provide the market the certainty and workability it needs to power that innovation.

Smart regulation benefits consumers, developers, and platforms by providing clear rules of the road that allow the benefits of crypto to shine.

It's time to update the system. As noted above, crypto brings with it tools – namely, an immutable, public ledger – that law enforcement does not have in traditional finance. Investigations on a blockchain are easier. *Applying the measures described here, and bringing as much activity onshore as possible, would likely create a more secure system* than the current traditional finance approach.

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. Safeguarding our platform from illicit activity 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.