Testimony of Alison Jimenez
House Sub-Committee on Digital Assets, Financial Technology, and Inclusion
Hearing: Crypto Crime in Context- Breaking Down the Illicit Activity in Digital Assets
November 15, 2023

Chairman Hill, Ranking Member Lynch, and distinguished Members of the Sub-Committee, thank you for the invitation to appear before you today to discuss illicit activity in digital assets.

Introduction

My name is Alison Jimenez. I am an economist and the president of Dynamic Securities Analytics, Inc., a private consulting firm that I founded in 2003 that focuses on compliance and litigation consulting on issues relating to financial crime and anti-money laundering ('AML').

In the course of my work, I advise AML software providers, conduct independent AML reviews for financial institutions, serve as an expert witness on financial crime and money laundering, provide training, and conduct research into financial crime and money laundering topics.

My research on money laundering has covered a range of issues from Ponzi schemes to Human Smuggling Finance to how the U.S. border closures during the Covid-19 pandemic impacted money laundering operations of Drug Trafficking Organizations.

Recently, much of my research has focused on the use of cryptocurrency in illicit finance. The topics of my research on cryptocurrency crime has included unregistered cryptocurrency exchanges, Suspicious Activity Reports filed by cryptocurrency exchanges, consumer complaints about cryptocurrency frauds and scam, illicit crypto activity occurring within Virtual Asset Service Providers, and national security issues relating to cryptocurrency. My crypto crime analysis has been featured in *American Banker*, the *Wall Street Journal*, and the *Financial Times*.

Valuable Features of Financial Products to Bad Actors

Before addressing cryptocurrency crime specifically, it is useful to understand how a bad actor evaluates financial products generally. When a bad actor wants to conduct a financial transaction, they will assess whether a financial product can move funds:

- far,
- fast,
- in large amounts,
- irreversibly,
- anonymously,
- and to a third-party.

There is no one feature that drives bad actors to a particular type of financial product. Anonymity is just one feature that bad actors weigh.

While a truckload of nickels and dimes is anonymous, it cannot be moved far or fast. Gift cards are also anonymous but usually have a dollar cap and are not ideal for moving a lot of value at once. For example, paying a $150 million dollar bribe to a foreign government official with gift cards, even with a $2,000 cap, would require roughly 75,000 gift cards.

Why do bad actors use cryptocurrency?

Cryptocurrency is attractive to bad actors because it has so many of the features they value in a financial product.

Blockchain based cryptocurrency transactions move seamlessly across international borders (*far*) and can be settled in minutes (*fast*). There is no cap on the value of cryptocurrency that can be transferred in a transaction (*in large amounts*). In most instances, a cryptocurrency transaction cannot be reversed once it has been added to the blockchain (*irreversibly)*. Cryptocurrency wallets are pseudonymous, meaning the true owner of the wallet may never be linked to a given wallet address (*anonymously)* and the same can be true for the recipient (*to a third-party*).

However, anonymity is not a priority for all bad actors using cryptocurrency. As is the case for many residing outside of the United States, especially within competitor nation-states, because it is difficult for our regulatory and legal systems to hold them accountable. Additionally, the anonymity, or even pseudonymity, of wallet addresses makes it challenging to determine when transactions are sending funds to another party or just to another wallet owned by the originator.

While some commentators argue that blockchain transparency makes cryptocurrency ill-suited for illicit finance. If we follow that logic, then:

- The weight and bulk of currency make cash ill-suited for illicit finance.
- The reversibility of wires makes it ill-suited for illicit finance.
- The dollar limit on Zelle transfers makes it ill-suited for illicit finance.
- The physical location of real estate makes it ill-suited for illicit finance.
- The names and addresses printed on checks make checks ill-suited for illicit finance.

However, as noted above, no one factor deters bad actors from finding ways to use financial products. Dismissing cryptocurrency as a useful tool for illicit finance just because some transactions are pseudonymously recorded on a blockchain is not wise. Nor is it borne out by cryptocurrency Suspicious Activity Reports (SAR), IC3 advisories, or CFPB consumer complaints.

What do we know about crypto crime?

My testimony focuses on three different data sources on cryptocurrency illicit finance: (1) Suspicious Activity Reports filed by financial institutions; (2) victim complaints; and (3) blockchain analytics.

1. SUSPICIOUS ACTIVITY REPORTS (SARS) FILED BY FINANCIAL INSTITUTIONS INDICATE PREVALENCE OF CRYPTOCURRENCY IN ILLICIT FINANCE.

My analysis of publicly available information regarding Suspicious Activity Reports involving cryptocurrency identified several insights into crypto crime.

- The number of SARs filed related to cryptocurrency is growing exponentially.[1] Over 92,000 cryptocurrency SARs were filed in 2021 reflecting transactions worth over $96 billion dollars.[2]
- Bad actors prefer to use cryptocurrency over many other financial products.[3] When adjusted for percentage of U.S adults using a given financial product, crypto SAR filings dwarf SARs filed relating to investment products and are gaining ground on U.S currency SARs. For example, there were 2.74 SARs per 1,000 Users of Crypto versus 0.18 SARS per 1,000 Users of Stocks. Even without adjusting for consumer adoption, there were more cryptocurrency SARs filed in 2021 than for all securities/investment products from 2014 through 2020.
- The dollar value of each cryptocurrency SAR hovers near $1 million dollars which is significantly greater than the dollar value of other products and industries.[4]
- Ransomware-related SARs filed in the second half of 2021 *exclusively* demanded payment in cryptocurrency. Ransomware SARs exemplifies the three prior points: the number of ransomware SARs is increasing dramatically, bad actors prefer payment in cryptocurrency, and the average dollar value of the bitcoin paid in ransom was over $900,000.[5]

Cryptocurrency-related SAR filings overwhelmingly contradict the thesis that bad actors don't use crypto.

2. THE BREADTH AND VOLUME OF VICTIM COMPLAINTS ILLUSTRATE THE MAGNITUDE OF THE ILLICIT ACTIVITY.

[1] https://securitiesanalytics.com/cryptocurrency-sars-what-do-we-know/
[2] Kevin O'Connor, FinCEN Section Chief- Virtual Assets and Emerging Technology. Association of Certified Financial Crimes Specialists webinar, "Russia Sanctions: The US Response. Crypto and Compliance", 4/20/202.
[3] https://securitiesanalytics.com/crypto-suspicious-activity-reports-vs-other-products-industries/
[4] Id.
[5] https://www.fincen.gov/sites/default/files/2022-11/Financial%20Trend%20Analysis_Ransomware%20FTA%202_508%20FINAL.pdf

Insights from Complaints Submitted to the FBI

The FBI's Internet Crime Complaint Center's ("IC3") mission is to provide the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning internet facilitated crime. IC3 analyzes and disseminates information for public awareness. To that end, the FBI has issued numerous consumer alerts about cryptocurrency scams including:

- **DeFi Exploits**: The FBI warns that cyber criminals are increasingly exploiting vulnerabilities in decentralized finance (DeFi) platforms to steal cryptocurrency, causing investors to lose money. The FBI reports that between January and March 2022, cyber criminals stole $1.3 billion in cryptocurrencies, almost 97% of which was stolen from DeFi platforms.
- **Fake Apps**: The FBI reported that fake crypto apps defrauded investors of more than $42 million between October 2021 and July 2022.
- **Crypto ATMS and QR Codes**: The FBI warned about scams leveraging cryptocurrency ATMS and QR Codes to receive payments from victims in online impersonation scams, romance scams, and lottery scams.
- **Liquidity Mining Scams**: The FBI states that liquidity mining scams has been responsible for over $70 million in losses since January 2019. Liquidity mining scams are also found in CFPB consumer complaints.
- **Impersonation of Law Enforcement**: The FBI warned of scammers impersonating law enforcement or government officials in attempts to extort or steal personally identifiable information. The scammers often demand payment via cryptocurrency ATMs.
- **Romance Scams/Pig Butchering**: The FBI received over 19,000 complaints related to online romance scams in 2022 with victims reporting over $735 million dollars in losses.

  The term "pig butchering" refers to the practice of fattening a hog before slaughter but in this context signifies a scamming technique of creating sense of intimacy with the victim before exploiting the victim via a cryptocurrency investment scam. Scam victims are often contacted via social media or "errant" text messages. The scammer on the other end of the message are often human trafficking victims who were lured to fake call center jobs, held against their will by organized crime groups, and forced to scam under the threat of violence.

  Homeland Security Investigations describes Pig Butchering as:

  > *an increasingly prolific financial fraud scheme, which combines elements of traditional romance and investment fraud whilst also targeting people trafficking and **modern slavery victims**. The typology generally (although not exclusively) is controlled by organized criminal gangs operating from Southeast Asia, including Special Economic Zones (SEZ) in countries like*

> *Myanmar, Laos, Cambodia and Thailand. In 2022, U.S. based victims alone lost approximately $3.3 billion dollars to crypto-related investment frauds.*[6]

- **Business Email Compromise and Second Hop Transfer**: The FBI reports that Business Email Compromise victims have unknowingly had their email hacked and wire instructions were altered by bad actors to instead wire funds to cryptocurrency exchanges. Another disturbing pattern is the "Second Hop Transfer" that the FBI describes as:

> *Second Hop Transfer uses victims of other cyber-enabled scams such as Extortion, Tech Support, and Romance Scams. Often, these individuals provided copies of identifying documents such as drivers' licenses, passports, etc., that are used to open cryptocurrency wallets in their name.*

Other IC3 cryptocurrency-related advisories include:

- Sextortion
- Cryptocurrency Scam Re-Victimization
- Human Trafficking to Scam Compounds Call Centers (Pig Butchering)
- Pig Butchering Cryptocurrency Scams
- Cryptocurrency Mining Scams
- Deepfakes and Stolen PII

Insights from CFPB Consumer Complaints

My analysis of CFPB consumer complaints identified traditional financial institutions frequently named in complaints involving digital assets, even though these firms may not offer cryptocurrency. For example, consumers alleged that their bank or fintech account was hacked and that the stolen funds were used to purchase cryptocurrency.[7]

The CFPB published an analysis of consumer complaints related to crypto-assets in November 2022.[8] From October 2018 to September 2022, the CFPB received more than 8,300 complaints related to crypto-assets with about 40% of the complaints listing frauds and scams as the main complaint.

3. INSIGHTS FROM BLOCKCHAIN ANALYTICS

Blockchain analytics has contributed to our understanding of crypto crime and has proven helpful to law enforcement in tracing blockchain-based illicit transactions.

[6] https://www.ice.gov/doclib/cornerstone/pdf/cornerstoneACAMS_SpecialIssue40_Apr21_2023.pdf
[7] https://securitiesanalytics.com/cfpb-cryptocurrency-complaints/
[8] https://files.consumerfinance.gov/f/documents/cfpb_complaint-bulletin_crypto-assets_2022-11.pdf

The efforts of blockchain analytic firms, coupled with examples of law enforcement successfully tracing cryptocurrency across the blockchain may have even caused bad actors to change *how* they use cryptocurrency. That is to be applauded. The days of publicly listing a static bitcoin wallet address to receive illicit funds may be over.

However, blockchain analytics does not change the *features* of cryptocurrency that are most attractive to bad actors: namely, the ability to move value far, fast, irreversibly…in large amounts. Additionally, when bad actors use the obfuscation methods discussed below, they may also evade attribution.

Limits of Blockchain Transparency

Many bad actors have changed how they transact with cryptocurrency on the blockchain to limit exposure to blockchain analytics and tracing.

On-chain obfuscation methods include:

- Using mixers
- Using De-Fi protocols as a mixer
- Transacting on "layer 2" protocols such as the bitcoin Lightning Network
- Hopping from one blockchain to another
- Creating new 'clean' wallets or addresses for each on-chain transaction
- Using privacy-enhanced cryptocurrencies
- Selecting blockchains with enhanced privacy features

Challenges to On-Chain Attribution

Attribution of a wallet address to a specific person or entity is challenging, especially for the private sector who lack access to off-chain data available to law enforcement or intelligence agencies.

Additionally, blockchain analytic firms do not always reach the same conclusions regarding attribution even when they are working from the same blockchain data. Finally, the attribution and tracing methodology used by blockchain analytics firms is often proprietary and unaudited.

Cryptocurrency Exchanges Internal Transactions Escape Blockchain Analytics

If all cryptocurrency transactions were an iceberg, the crypto transactions subject to blockchain analytics is the small portion above the waterline.

Most cryptocurrency transactions occur within crypto exchanges. Crypto exchanges internally match buyers and sellers. Exchanges also act as market-makers, stepping in as a counterparty when a buyer/seller is unavailable. These off-chain transactions escape traceability and blockchain analytics.

Researchers estimated that bitcoin transactions within exchanges to be ten times the volume of transactions executed on the blockchain:

> *On-chain transactions, however, constitute only a small share of the universe of all Bitcoin trades, most of which are "off-chain" utilizing some form of exchange, some heavily regulated, some not so much.*[9]

Internal Ledgers at Crypto Exchanges.

A crypto exchange's internal transactions are not recorded on the blockchain. Instead, these off-chain transactions are recorded on the exchange's internal ledger.

Bad actors can use cryptocurrency but evade creating a blockchain record of transactions by simply conducting transactions within an exchange. As demonstrated by SAR filings by Virtual Asset Service Providers (VASPs), IC3 and CFPB complaints, and criminal indictments, this is in fact occurring.

Illicit Customer Activity Within Cryptocurrency Exchanges

My analysis of nine enforcement actions against VASPs involving Suspicious Activity Reports found that darknet market activity was the most cited suspicious activity.[10] Other sources of illicit funds flowing through the VASPs included: funds from sanctioned entities/regions, Child Sexual Assault Material (CSAM), money laundering, drug trafficking, ransomware, unregistered MSBs and/or crypto mixers, terror finance, and other fraud.

Illicit Activity by Cryptocurrency Exchanges

Cryptocurrency exchanges and other types of VASPs, such as mixers and bitcoin ATMs, have also directly engaged in illicit financial activity using cryptocurrency.

Internal exchange ledgers of cryptocurrency transactions have been sloppy or outright fraudulent from the very beginning. Mt. Gox, one of the first cryptocurrency exchanges, allegedly failed to accurately record internal customers transactions, and stole crypto from customers.

Cryptocurrency exchanges have also engaged in market manipulation, wash trading, insider trading, and a host of other crimes.[11] Perhaps even more concerning is that sanctioned countries are operating cryptocurrency exchanges.[12]

[9] https://www.nber.org/papers/w29337
[10] https://securitiesanalytics.com/crypto-suspicious-activity-report-enforcement-actions/
[11] https://securitiesanalytics.com/fraud-within-crypto-companies/
[12] https://securitiesanalytics.com/sanctioned-countries-are-operating-crypto-exchanges/

> *"We've got sanctioned countries setting up cryptocurrency exchanges that are being used to facilitate the transfer of U.S. dollars over to those sanctioned countries. I've seen those in the millions, and potentially in the billions."* – Jack McDonald, IRS-CI, ABA/ABA Financial Crimes Enforcement Conference, December 2022.

Flawed comparisons of crypto crime to fiat

Putting crypto crime into context is a worthwhile endeavor but making invalid comparisons only confuses the issue.

Hopefully we can agree that the comparison below is nonsense:

> Alice drinks 2% milk.
>
> Bob puts 98% unleaded gasoline in his car.
>
> Bob's percentage is 49 times greater than Alice's!

Yet, statements like this are routinely used when discussing cryptocurrency's use in illicit finance versus traditional financial products.

Commentators often erroneously compare a UN estimate of the value of illicit proceeds ranging 2% to 5% of global GDP to numbers published by blockchain analytics vendors that report transactions involving illicit address are less than 1% percent of all digital asset transaction volume. Some commentators extrapolate from the invalid comparison to suggest that "criminals don't like crypto."[13]

Here are a few reasons why this comparison is flawed:

- Blockchain analytics illicit transactions only include "known" or "attributed" on-chain transactions while the UN's estimate was of *all* illicit proceeds, not just proceeds clearly "attributed" to criminals.
- The UN estimated the proceeds of crime, not the means of payment. The means of payment could have been real estate, oil, stock, jewelry, bartering of drugs for weapons, or government issued currency (fiat).
- Blockchain analytics vendors divide their illicit crypto transaction amount by all cryptocurrency transaction volume. Cryptocurrency transaction volume is inflated in several ways including: bad actors creating thousands of transactions to obscure fund movement, leveraged trading, rampant wash-trading, and moving cryptocurrency between wallets without any meaningful economic activity.
- Blockchain analytics calculations divides "known" illicit transactions by "all" cryptocurrency transactions. The denominator, "all crypto transactions", includes *unidentified* illicit activity, licit transactions, and unclassified transaction. Commentators

[13] Couvee, Koos. "Cryptocurrency Research Firms Vastly Underestimate Illicit Payments, Critics Claim", ACAMSToday, 6/29/23.

often incorrectly interpret this data to only include the binary options of illicit or licit activity. Additionally, when transactions are attributed a regulated exchange, blockchain analytics often cannot determine if illicit crypto was involved.

- Global GDP and "all cryptocurrency transaction volume" are not interchangeable and do not measure the same thing. Global "transaction volume" is orders of magnitude greater than Global GDP.

In summary, blockchain analytics, while helpful in certain situations, cannot and does not provide the complete picture of the use of cryptocurrency in illicit finance.

Illicit Finance by "Ancillary" Cryptocurrency Entities

One final topic worth addressing in my testimony is the issue of cryptocurrency illicit finance by cryptocurrency miners/validators.

Cryptocurrency miners are often viewed as the unexciting plumbing behind crypto, with a simple business of earning new coins from processing transactions.

However, my analysis has found dozens of ways that cryptocurrency miners/validators have been involved in illicit activity including[14]:

- sanctioned entities mining cryptocurrency to raise funds
- theft crimes (ex. stealing computing power via malware)
- facilitating money laundering or theft by others (ex. validating transactions from known illicit sources)
- corruption (ex. paying bribes for electricity subsidies)
- investment scams
- cryptocurrency market manipulation.

National security concerns have also risen from cryptocurrency mining. For example, the Department of Justice reported that Russian government-backed hacking activities were partially funded via bitcoin mining.[15] Recently, the *New York Times* reported on national security concerns relating to Chinese-owned bitcoin mining operations in the United State.[16]

Recommended Actions:

1) FinCEN should regularly publish the number of cryptocurrency-related SARs.
2) The SAR form should be updated to include cryptocurrency as a financial product/instrument.

[14] https://securitiesanalytics.com/cryptocurrency-miners-crime-let-me-count-the-ways/
[15] https://www.justice.gov/archives/sco/file/1373816/download
[16] https://www.nytimes.com/2023/10/13/us/bitcoin-mines-china-united-states.html

3) The SAR form should be updated to specifically categorize SARs filed by cryptocurrency-related institutions.
4) Proposed legislation should consider cryptocurrency illicit finance by cryptocurrency miners, validators, and mining/validating pools.
5) Proposed legislation should not provide weaker oversight to stablecoins given their growing use in illicit finance.