

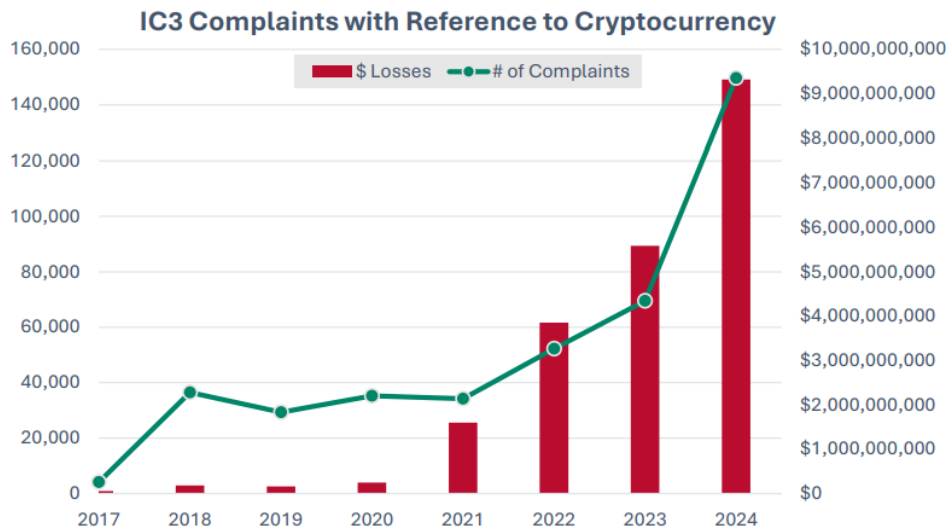
## Boom Times for Crypto Crime

By Amanda Fischer | *Policy Director & COO*

May 6, 2025

The Federal Bureau of Investigation’s Internet Crime Report is perhaps the best source of data on cyber crime. The [2024 report](#), released on April 23, 2025, found:

- **\$16.6 billion of cyber crime** in 2024, **56% of which involved crypto**;
- **\$9.3 billion in total cryptocurrency-related losses** in 2024, a **66% increase** from 2023;
- **140,000 complaints** referencing cryptocurrency came to the FBI from harmed individuals in 2024, a **more than doubling** of complaints versus 2023;
- **Individuals over the age of 60 were most affected** by crypto-related fraud, with roughly **33,000 complaints** and **\$2.8 billion** in losses;
- Complaints related to **cryptocurrency ATMs/kiosks increased 99%** in 2024 compared to 2023, with **losses increasing 31%**; and
- **Complaints related to extortion or “sextortion” (manipulating photos/videos to intimidate victims) increased by 59%** in 2024 versus 2023, with **losses increasing 9%**.



<sup>20</sup> Accessibility description: Chart outlines cryptocurrency complaints in 2024: 149,686 complaints; \$9.3 billion in losses; 66% increase in loss; largest age group to report is 60+.

<sup>21</sup> Not all complaints include an associated age range—those without this information are excluded from this table. Please see Appendix C for more information regarding IC3 data.

<sup>22</sup> Chart outlines the number of cryptocurrency related complaints from 2017 to 2024.

The FBI concludes that “cryptocurrency has become an enticing means to cheat investors, launder proceeds, and engage in other illicit schemes.”

## Administration Actions to Enable Crypto Crime

While crypto crime surged over the last year, the Administration has unleashed a flurry of actions to enable such crime by making it harder to detect, investigate and prosecute.

- **Department of Justice Disbands Crypto Enforcement Unit:** within 24 hours of the inauguration, the DOJ [reassigned](#) its lead civil servant attorney who prosecuted crypto crimes and later [disbanded](#) its entire National Cryptocurrency Enforcement Team, which had previously investigated and brought cases against money launderers—including a case against Binance and its founder Changpeng Zhao (CZ), who plead guilty and served time in jail. During the Biden Administration, lawmakers such as House Financial Services Committee Chairman [French Hill](#), Senator [Cynthia Lummis](#) and Congressman [Richie Torres](#) chided government law enforcement agencies for not prosecuting Binance's crypto crimes fast or vigorously enough. Now, the prosecutors that do that work have been reassigned altogether.
- **Department of Justice Non-Prosecution of Crypto Memo:** in April 2025, the DOJ [announced](#) that it would no longer investigate or bring money laundering or illicit finance cases against crypto firms like trading platforms, digital wallets or online money laundering services known as “mixers” and “tumblers.” While the DOJ says that they will instead prioritize bringing cases against *individuals* who use crypto company services to engage in crimes, this supposed strategy defies credibility and will only allow crypto crime to proliferate. It is akin to the cops announcing that they'll pursue street level drug dealers but not the banks that help drug cartels launder money. Crypto crime is enabled by companies that look the other way when individuals systematically use their services for illicit purposes.

Specifically, trading platforms enable and even encourage criminal behavior by having weak or non-existent anti-money laundering compliance programs. In fact, in the case of Binance, the trading platform and its founder CZ plead guilty to [actively soliciting](#) customers to create offshore entities to evade U.S. anti-money laundering laws. While the DOJ announcement left open the possibility that they'd enforce the law against companies that “willfully” violate it, the memorandum [represents](#) “a marked shift from the previous Administration.” Further, it is very difficult for prosecutors to prove malicious intent for committing money laundering violations when they're not enforcing threshold registration or policies and procedures requirements to begin with. And the crypto industry is certainly interpreting the policy change as a boon for them. Just one day after the DOJ issued its memo, CZ of Binance [posted](#) on X.com about it with a shrug emoji. When someone [replied](#) to CZ that he suffered “the burden of being early,” CZ responded with a laughing crying emoji, underscoring the irony that this law enforcement amnesty came too late for him and Binance.


Finally, the non-prosecution of mixing and tumbling services likewise raises huge national security concerns, as DOJ previously [noted](#) that “mixers...[serve] as safe havens for laundering criminally derived funds, including the proceeds of ransomware and wire fraud” by scrambling up crypto to conceal the sources and movement of funds.

- **Department of Justice Steps Away from Other Law Enforcement:** in addition to the above actions related specifically to cryptocurrency, the President also signed an [Executive Order](#) “pausing” enforcement of the Foreign Corrupt Practices Act and is reportedly considering [shutting down](#) the branch of DOJ that enforces consumer protection laws.
- **Securities and Exchange Commission Drops Lawsuits, Becomes Crypto Crime Cheerleader:** as Better Markets previously [documented](#), the SEC has been dropping and “pausing” a host of lawsuits against crypto companies, including those engaged in fraud. This is despite the fact that virtually every independent Article III federal judge across the country has ruled against the crypto industry, often in lengthy and detailed decisions that make it clear that crypto’s positions lack a valid legal basis.
- **Securities and Exchange Commission Slashes Crypto Enforcement Staff:** the SEC also dismantled the crypto unit in its Division of Enforcement, reassigning and demoting key personnel. All told, approximately 20 of the 50 staff in the unit have [reportedly](#) been moved out of their prior jobs. Additionally, the SEC took action to [strip enforcement attorneys of subpoena authority](#) for documents and testimony, requiring a cumbersome vote of the full Commission in order for investigations to move forward.

## Debunking Crypto Myths

The crypto industry and their apologists in Congress have cited a number of myths to dismiss the prevalence of crypto-facilitated crime.

- **Myth: New Congressional Legislation Will Help Stop Crime**
  - **Fact – the Legislation Just Restates Existing Law that Crypto Firms Already Flout:** stablecoin issuers and crypto firms such as trading platforms are generally already registered as state money service businesses and are required to comply with federal anti-money laundering laws. Pending stablecoin and crypto market structure legislation simply restates existing law and does not apply stronger standards than those that already exist. Crypto firms already flout those laws, as evidenced by [numerous enforcement actions](#) during the Biden Administration. New crypto legislation that restates existing obligations under the law is meaningless when the Trump Administration announced the intention not to enforce the law. It defies logic that the Congress would integrate stablecoins into the mainstream banking system during this law enforcement amnesty period when one crypto trade publication [called](#) stablecoins “the kingpin of illicit crypto activity” and a crypto data firm found that stablecoins were involved in [63% of crypto crimes](#).



Finally, in certain instances, legislation creates new, ambiguous and overbroad definitions of “decentralized finance,” or DeFi, which would allow certain firms to escape anti-money laundering legal obligations under the guise of “just being open source code.”

Nothing in pending congressional legislation—including recent changes to the GENIUS Act—address the prevalence of money laundering and legal non-compliance in the crypto and stablecoin industries.

- **Myth: Criminals Launder Money With Cash, Real Estate, Art and Cases of Wine, So Crypto Crimes Are Not Unique and No Big Deal.**

- **Fact – Crypto is Uniquely Suited to Crime:** yes, money laundering existed before the existence of crypto and continues to exist outside the use of crypto. But crypto is uniquely suited for money laundering given the ease with which criminals can transmit large sums of value. Cash, art and cases of wine are all physically bulky and require huge networks of people to transport, whereas crypto is borderless lines of code requiring just a few skilled hackers to move value. In the words of one [report](#) citing a Treasury Department study, “cryptocurrency remains the remains the payment method of choice for criminal ransomware actors.” There is a reason why a [reported](#) 98% of ransomware payments demanded by criminals was in the form of Bitcoin and not, say, Rolex watches or Picasso paintings.


Additionally, while crypto firms claim that [less than 1% of crypto activity](#) is related to illicit finance, Suspicious Activity Reporting from a limited subset of firms demonstrated that [nearly 12% of crypto activity](#) triggered a SAR being reported to law enforcement.

National security experts have also [testified](#) that proprietary data on the use of crypto in crimes is drastically underreported. Because such private data only counts on-chain activity and not off-chain activity (or crypto trading that occurs internally on firms’ databases and not on blockchains), they miss significant incidences of crime.

Additionally, the admonition to focus on money laundering via assets like real estate rings hollow when the Trump Administration has [separately suspended](#) enforcement of a bipartisan law meant to crack down on the use of shell companies to launder money.

- **Myth: Blockchains Are Public and Traceable So Money Laundering With Crypto is Actually Harder To Get Away With.**

- **Fact – Blockchains Paint an Incomplete Picture:** again, national security experts have [stated](#) that proprietary firms that report crypto crime understate the problem because they do not report on off-chain activity, or crypto trading that occurs off of



blockchains. Because significant amounts of illicit activity happen at crypto trading platforms, which internally match customer orders but don't report that volume on the blockchain, crime is underreported and can't be traced on a blockchain. In fact, one study [estimates](#) that when it comes to Bitcoin, this off-chain transaction volume is at least 10 times greater than on-chain transaction volume.

Additionally, the use of crypto “mixers,” or software that is designed to obfuscate flows of funds by scrambling crypto payments and addresses, limit the effectiveness of blockchain data to trace illicit transactions.

The result is that crypto is a very effective means of money laundering. As one crypto security firm [noted](#), “North Korea has developed a powerful and sophisticated capability to not only breach target organizations and steal cryptoassets, but also to launder these proceeds through thousands of blockchain transactions.” Even if you trust the [accounting](#) from the Bybit crypto exchange, which was subject to a \$1.5 billion hack by North Korea in order to fund its nuclear program, nearly 28% of the hacked funds remain untraceable and unfrozen. That's more than \$420 million for a few minutes of work.

## Conclusion

The FBI's own data suggests that crypto crime is a huge and growing problem. At the same time, the Administration is walking away from its legal obligation to crack down on crime, instead acting as a cheerleader for the industry. Contrary to talking points from the crypto industry, crypto is a uniquely effective means to launder money. Further integrating these assets into Americans' wallets and our nation's banking system is a bad idea, especially at a time when law enforcement is abdicating its duty to protect consumers and our national security.



Better Banks | Better Businesses  
Better Jobs | Better Economic Growth  
Better Lives | Better Communities

**Better Markets** is a public interest 501(c)(3) non-profit based in Washington, DC that advocates for greater transparency, accountability, and oversight in the domestic and global capital and commodity markets, to protect the American Dream of homes, jobs, savings, education, a secure retirement, and a rising standard of living.

Better Markets fights for the economic security, opportunity, and prosperity of the American people by working to enact financial reform, to prevent another financial crash and the diversion of trillions of taxpayer dollars to bailing out the financial system.

By being a counterweight to Wall Street's biggest financial firms through the policymaking and rulemaking process, Better Markets is supporting pragmatic rules and a strong banking and financial system that enables stability, growth, and broad-based prosperity. Better Markets also fights to refocus finance on the real economy, empower the buy-side and protect investors and consumers.

For press inquiries, please contact us at [press@bettermarkets.com](mailto:press@bettermarkets.com) or (202) 618-6430.



[SUBSCRIBE](#) to Our Monthly Newsletter

FOLLOW US ON SOCIAL

