In 2019, a doctor's office in the Mahoning Valley in Ohio experienced a disturbing attack: hackers locked the office computers, making them unusable. They even faxed over a ransom note, promising to unlock the computers if the practice turned over $75,000—in Bitcoin.

Not long ago, a Syrian group tied to al-Qaeda put out a call for donations to help buy weapons. Their social media post said that supporters should "donate anonymously with cryptocurrency."

"Donate anonymously."

A week ago today, the Justice Department announced an indictment of two individuals who allegedly turned the profits of scams into cryptocurrency. Then they'd send the crypto overseas, where it could be turned back into cash.

This Committee has been examining digital assets to learn how they work and the risks they create for consumers and the financial system. We've also considered how digital assets can put workers' hard-earned money at risk.

We're here today because crypto also can be used to make it easier to commit crimes – facilitating illicit finance, terrorism, and other forms of criminal activity, and threatening our national security. Bad actors around the world—from hackers, scammers, and drug traffickers, to terrorist groups and pariah regimes—have sought digital assets to facilitate their crimes and intimidation.

In October 2020, under the last Administration, the Justice Department concluded that, "cryptocurrency technology plays a role in many of the most significant criminal and national security threats that the United States faces."

To be sure, criminals have tried to cover their tracks for years with sham accounting and banks that looked the other way. But there's a simple reason that crypto appeals to crime rings and scam artists.

The dollar has safeguards to protect against crime and illicit activity. Companies that deal with real money are required to know their customers, and report suspicious transactions. They need to keep records.

And even when crypto companies are covered by the law, too many don't play by the same rules—especially offshore crypto operators that aren't subject to U.S. law.

Shady crypto companies that fail to adequately monitor activity on their platforms all but give criminals a green light.

Digital assets make it easier to move money under pseudonyms. They make it easier for money launderers to use webs of transactions across the globe to cover their tracks. And that makes it harder for law enforcement to trace illicit funds.

And, the Financial Crimes Enforcement Network— FinCEN, the Treasury bureau charged with safeguarding our financial system from abuse—warned last week that Russian actors could even use crypto to get around sanctions.

So sophisticated bad actors can use digital assets in ways that, if they were using dollars, would likely raise red flags and get them stopped in their tracks.

Last year, FinCEN fined a crypto exchange $100 million. For six years, the only identification the company bothered to get from customers was an email address. That no-questions-asked approach enabled more than $200 million in suspicious transactions.

But the problem isn't only shoddy compliance. It's more fundamental.

We hear all the time about how "innovative" cryptocurrency is. But criminals innovate, too. Crypto allows money launderers and terrorists to do things they never could have done with dollars. There's a whole new vocabulary to explain cryptocurrency illicit activity.

Take what's known as "chain hopping." That's when someone launders money by changing funds from one cryptocurrency ecosystem to another, to make it harder to track.

Or look at so-called "rug pulls." That's when you set up a sham digital asset project online, raise as much money as you can, scamming investors, and then run off with all the cash.

Then there's Hydra, the world's largest "darknet." It's an online black market for drugs, stolen credit card numbers, and cyberattack services, all enabled by crypto.

Our laws and law enforcement agencies need to keep pace with bad actors that will exploit every opportunity.

And so far, with lax rules and little oversight, we've given them plenty of those opportunities.

Crypto lets money launderers, hackers, and rogue regimes invent new ways to hide and move money in the dark. It lets hackers and scammers create new ways to steal or defraud. And if we allow them get out ahead of us, our safety and security will be at risk.

Law enforcement is doing what it can. They use techniques to stop cybercrime that didn't exist 30 years ago. Financial regulators leverage new data and resources to expose fraud and manipulation in our markets.

Crypto technology also embeds information that allows law enforcement and national security officials to track and trace where it's been – though not necessarily who owns it. That's where the tough new money laundering and beneficial ownership law we enacted last year will help.

But as these problems continue to grow, we can't sit on the sidelines. We need to take a clear-eyed look at how these assets can endanger consumers and our security.

Last month the FBI announced the creation of a new unit dedicated to tracking down illicit crypto. The Justice Department is dedicating more resources and staff to cracking down on crime using digital assets.

We need to take a whole-of-government approach to the problem, if we're going to keep up with crypto in illicit finance.

President Biden understands that. His executive order on crypto assets last week will drive progress on this issue. It will jumpstart a coordinated strategy from law enforcement and regulators to fight bad actors who want to use crypto.

Ultimately, we can't just sit back and watch cybercriminals, rogue regimes, terrorists, and others create a shadow financial system that works for them.

The financial system should work for American families and small businesses. Everything we do on this Committee has that goal in mind. That means that we cannot let abuses of digital assets endanger our financial and national security.

As crypto technology evolves, this Committee must continue to work together to craft a way forward on these crypto policy issues. The stakes are high, and the American people are counting on us.