The Digital Asset Anti-Money Laundering Act of 2023
Senators Elizabeth Warren and Roger Marshall

The Treasury Department, Department of Justice, the Federal Bureau of Investigation, and other national security and law enforcements experts have warned that digital assets are increasingly being used for money laundering, ransomware attacks, theft and fraud schemes, trafficking, terrorist financing, and other crimes. Rogue nations like Iran, Russia, and North Korea – which has emerged as one of the world's most prolific crypto-criminals, stealing $1.7 billion in digital assets in 2022 alone – have turned to digital assets to evade sanctions and fund illegal weapons programs. It is estimated that half of the DPRK's missile program is funded by cybercrime and digital assets. Ransomware attackers, which almost exclusively demand payment in digital assets, hit more than 2,400 local governments, schools, and hospitals in the U.S. last year. Fentanyl chemical producers in China are increasingly using crypto to sell their products to cartels in the U.S. – last year, these producers accepted over $30 million in crypto payments, selling enough precursor chemical to produce an estimated $50 billion in illicit drug products like fentanyl and methamphetamine. Overall last year, illicit use of digital assets hit a record high of at least $20 billion, with 44% of those transactions affiliated with sanctioned entities.

As the international Financial Action Task Force warned, "gaps in the global regulatory system have created significant loopholes for criminals and terrorists to abuse," risking the creation of a "virtual safe haven for the financial transactions of criminals and terrorists." The *Digital Asset Anti-Money Laundering Act* would mitigate the risks that digital assets pose to our national security by closing loopholes and bringing the digital asset ecosystem into greater compliance with the anti-money laundering and countering the financing of terrorism (AML/CFT) frameworks governing the greater financial system.

Specifically, the *Digital Asset Anti-Money Laundering Act* would:

- Extend Bank Secrecy Act (BSA) responsibilities, including Know-Your-Customer requirements, to digital asset wallet providers, miners, validators, and other network participants that may act to validate, secure, or facilitate digital asset transactions.

- Address a major gap with respect to "unhosted" digital wallets – which allow individuals to bypass AML and sanctions checks – by directing FinCEN to finalize and implement its December 2020 proposed rule, which would require banks and money service businesses (MSBs) to verify customer and counterparty identities, keep records, and file reports on certain transactions involving unhosted wallets or wallets hosted in non-BSA compliant jurisdictions.

- Direct FinCEN to issue guidance to financial institutions on mitigating the risks of handling, using, or transacting with digital assets that have been anonymized using digital asset mixers and other anonymity-enhancing technologies.

- Strengthen enforcement of BSA compliance by directing Treasury to establish an AML/CFT examination and review process for MSBs and other digital asset entities with BSA obligations and directing the Securities and Exchange Commission and Commodity Futures Trading Commission to establish AML/CFT compliance examination and review processes for the entities they regulate.

- Extend BSA rules regarding reporting of foreign bank accounts to include digital assets by requiring United States persons engaged in a transaction with a value greater than $10,000 in digital assets through one or more offshore accounts to file a Report of Foreign Bank and Financial Accounts (FBAR) with the Internal Revenue Service.

- Mitigate the illicit finance risks of digital asset ATMs by directing FinCEN to ensure that digital asset ATM owners and administrators regularly submit and update the physical addresses of the kiosks they own or operate and verify customer and counterparty identity.