Non-Paper on U.S. Action Against CVC Mixers

- On October 19, the Financial Crimes Enforcement Network (FinCEN), the financial intelligence unit of the United States, issued a notice of proposed rulemaking (NPRM) naming convertible virtual currency (CVC) mixing as a class of transactions of primary money laundering concern.

- The term "convertible virtual currency" or CVC, means a medium of exchange that either has an equivalent value as currency, or acts as a substitute for currency, but lacks legal tender status. Although Bitcoin has legal tender status in at least two jurisdictions, the term CVC includes Bitcoin for the purpose of this proposed rule.

- This proposed rule is not a sanction. It is expected to bring greater transparency to CVC mixing and protect against related threats to the U.S. financial system.

- "CVC mixing" entails the facilitation of CVC transactions in a manner that obfuscates the source, destination, or amount involved in one or more transactions. Because CVC mixing is intended to make CVC transactions untraceable and anonymous, CVC mixing is ripe for abuse by, and is frequently used by, illicit foreign actors that threaten the security of the United States and the U.S. financial system. By obscuring the connection between the CVC wallet addresses used to receive illicit CVC proceeds and the CVC wallet addresses from which illicit CVC is transferred to CVC-to-fiat exchangers, CVC mixing transactions can play a central role in money laundering.

- CVCs can be used for legitimate and innovative purposes. However, it is not without risks. In particular, the use of CVC mixing to anonymize illicit activity undermines the legitimate and innovative uses of CVCs.

- In the view of the United States, CVC mixing transactions are frequently used by criminals and state actors to facilitate a range of

illicit activity, including money laundering, sanctions evasion and weapons of mass destruction (WMD) proliferation by the DPRK, Russian-associated ransomware schemes, and illicit darknet markets. CVC mixing often involves foreign jurisdictions because persons who facilitate or engage in CVC mixing transactions are often located abroad, including notable recent CVC mixing by DPRK actors, Russian ransomware actors, and buyers and sellers on Russian darknet markets.

- This NPRM highlights the risks of the extensive use of CVC mixing services by a variety of illicit actors throughout the world and proposes a rule to increase transparency around CVC mixing. The proposed rule would require covered financial institutions to report information about a transaction when they know, suspect, or have reason to suspect it involves CVC mixing within or involving jurisdictions outside the United States.

- The United States supports innovation and advances in digital assets and distributed ledger technology for financial services. We must also consider the substantial implications that such technology has for national security and mitigate the attendant risks for consumers, businesses, national security, and the integrity of the broader U.S. financial system.

- The global nature of the problem is further demonstrated by the fact that no CVC mixers are currently registered with FinCEN. CVC mixers are required to register with FinCEN if they do business as money transmitters wholly or in substantial part within the United States. To the extent foreign CVC mixers are operating beyond United States jurisdiction, they are not subject to U.S. regulations that require financial institutions to, among other things, know the identity of their customers and report suspicious activity to FinCEN.

- As part of the NPRM, FinCEN is proposing to use special measure number one under Section 311 of the USA PATRIOT Act to require

covered financial institutions to implement certain recordkeeping and reporting requirements on transactions that covered financial institutions know, suspect, or have reason to suspect involve CVC mixing within or involving jurisdictions outside the United States.

- This additional transparency would serve two purposes. First, it would support money laundering investigations by law enforcement and regulators, including cases against DPRK and Russian cybercriminals that pose a threat to U.S national and financial system security. Second, it would highlight the risks and deter illicit actors' use of CVC mixing services, including by foreign state-sponsored or affiliated cyber actors' laundering proceeds of CVC theft to facilitate WMD proliferation, ransomware networks' laundering of ransoms, and obfuscation of transactions associated with the use of illicit darknet markets.

- The existing risk-based approach to AML/CFT compliance used by covered financial institutions already largely encompasses the information FinCEN is requesting. While the information is available to covered financial institutions, at present it is not universally reported to FinCEN. Although covered financial institutions possess customer information and can identify when their customers engage in a covered transaction, this proposed rule would compel covered financial institutions to attribute a covered transaction to the involved customer(s) and report this information to FinCEN.

- FinCEN is requesting public feedback on the proposed rule, and interested parties, including foreign governments, can comment on the rule through the online Federal Register (link in attachment) through January 22, 2024.