ErisX

January 4, 2021

Via Federal E-Rulemaking Portal and Via email: frc@fincen.gov

Policy Division
Financial Crimes Enforcement Network
P.O. Box 39
Vienna, VA 22183

Re: FinCEN Docket Number FINCEN-2020-0020, RIN 1506-AB47, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets"

Dear Sir/Madam:

ErisX appreciates the opportunity to submit this letter in response to Department of the Treasury, Financial Crimes Enforcement Network's ("FinCEN") Notice of Proposed Rulemaking regarding "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets" (the "NPRM").

About ErisX

ErisX is a unified platform for spot and regulated futures on cryptocurrencies.

Our futures market for physically delivered bitcoin and Ether contracts is regulated under the jurisdiction of the Commodity Futures Trading Commission (CFTC). On the Federal level, we hold, respectively, Designated Contract Market (DCM), and Derivatives Clearing Organization (DCO) licenses. Eris Exchange is the entity which holds the DCM license and Eris Clearing is the entity that holds the DCO license and clears cryptocurrency futures contracts traded on our regulated derivatives exchange. Both entities comply with relevant Core Principles under the Commodity Exchange Act including, among other things, establishing standards and procedures to protect members and participant funds and eliminate counterparty risk.

From inception, ErisX has applied the CFTC Core Principles (for both trading and clearing) to the ErisX Spot Market as a matter of best practice. Through Eris Clearing, the ErisX Spot Market is subject to certain state licensing requirements, is registered with FinCEN as an MSB, and operates in NY pursuant to a license to engage in virtual currency business activity by the New York State Department of Financial Services.

ErisX's management team is composed of experienced industry practitioners and includes senior industry leaders with backgrounds and operating experience spanning multiple regulated asset classes and global jurisdictions. ErisX's investors represent a diverse group of industry participants, including broker-dealers and futures commission

Comments

ErisX supports the important goals of FinCEN in combating money laundering, terrorist financing, and other illicit acts. As evidenced by our voluntary and early adoption of the CFTC Core Principles to our spot market (including market and trade practice surveillance) in addition to full implementation of the CFTC Core Principles to our futures market and clearing infrastructure--as required by law, we believe that detecting and preventing bad actors from utilizing blockchain and distributed ledger technology is both the right thing to do and essential to the long-term growth and success of the industry.

ErisX has several concerns with the NPRM, and in addition to supporting the comment letter submitted by the Chamber of Digital Commerce, our concerns are indicated below. While ErisX is a hosted wallet provider, we believe unhosted wallets are an important innovation and part of the value proposition for digital assets.

The NPRM proposes to create a bifurcation in the digital currency industry and treat unhosted wallets as hostile. By requiring increased due diligence, reporting and recordkeeping with regard to transactions involving unhosted wallets, the NPRM implies illegitimacy and wrongful conduct for those users that elect to use one form of wallet technology or solution over another. The conclusions in the NPRM are incongruous; and the cash equivalent of requiring all purchasers of traditional billfolds and/or purses to submit ownership information to a federal registry and submit to certain tracking protocols. Blockchain technology, on which all hosted and unhosted wallets operate, already provide surveillance, tracking, and transaction reconstruction tools that are well-beyond tools available for fiat currencies. We therefore encourage development of a more tailored solution than that proposed in the NPRM, and likely a risk-based solution that results from current SARs filings.

The NPRM proposes to require Banks and MSBs to verify and report ownership information for unhosted wallets when such information is not readily available or associated with unhosted wallets in a verifiable manner. Ownership of unhosted wallets cannot be known since a golden record of such information does not exist in any form. (This has given rise to vendor solutions that attempt to compile this information from various sources.) Given this limitation, Banks and MSBs must reasonably presume that whoever controls an unhosted wallet is also the owner, or must rely on self-reporting of the ownership information without certain methods of verification. If the premise of the NPRM is correct, that unhosted wallets must be

subject to increased due diligence due to presumed wrongful conduct, then reliance on self-reporting of ownership information is likely to result in deliberately inaccurate ownership information reported for unhosted wallets that are used for illegitimate purposes, with increased scrutiny and hurdles for those unhosted wallets that are used for legitimate purposes and are reported accurately. The resulting burden on the industry from compliance with the NPRM is likely severely increased for Banks, MSBs, and those unhosted wallets that operate legitimately, in exchange for questionable or unreliable data for those wallets that are of concern to the drafters of the NPRM.

This leads to concerns regarding general data security for reported information. The NPRM, if implemented as drafted, will result in multiple sources (Banks and MSBs) reporting a treasure trove of information (with low reporting thresholds) to a single destination, where it is susceptible to cyber attack, leakage, or digital intrusion or hacking. Recent reports of hacked and leaked information (including SARs reports, personally identifiable information, Federal agency files) and compromised vendor systems, call into question the soundness of creating an attractive target--or "honeypot." We believe (i) that due to potential resulting liability for reporting entities, safe harbor provisions should be extended to include all proposed reporting under this NPRM; and (ii) this data security risk is real and should be addressed, mitigated, or accounted for in the cost-benefit analysis.

Lastly, the costs associated with compliance with the NPRM are likely to be significant, especially for small entities that make up a majority of this developing industry (we estimate there will be software development costs for proprietary software; increased storage costs; increased vendor costs for updated software, alerts, storage, reporting; and overall costs for unanticipated fines). Additionally, if the approach undertaken in the NPRM is not adopted internationally, participants in this global industry will utilize markets in less intrusive jurisdictions and innovative entities will also establish in less restrictive jurisdictions to avoid the increased costs of compliance and stifling regulation. This loss of opportunity, innovation, and market participants is likely to be significant, and promote the use of the international markets at the expense of the markets here in the United States.

ErisX appreciates the opportunity to provide this public comment.

Sincerely,

/s/ Thomas Chippas
Thomas Chippas
CEO