



V A S P n e t .

Counterparty DASP Due Diligence

VASPnet's Response to Treasury's GENIUS
ACT Illicit Finance Report

24 June 2026

Treasury's report identifies an off-chain control gap

The U.S. Department of the Treasury's [report to Congress on innovative technologies to counter illicit finance involving digital assets](#) is an important contribution to the next phase of digital asset AML/CFT and sanctions controls.

VASPnet agrees with the recognition by Treasury on the role that artificial intelligence, digital identity, blockchain monitoring and analytics, APIs, information sharing and other technologies can play in detecting, preventing and disrupting illicit finance. It also highlights a number of risks that have become familiar across the digital asset ecosystem, including sanctions evasion, ransomware, DPRK cyber activity, scams, fraud, misuse of mixers and tumblers, and the abuse of services operating from jurisdictions with weak or non-existent AML/CFT obligations.

However, the report also points to a control gap that deserves further attention. Many of the risks identified by Treasury are not only on-chain risks, but also off-chain counterparty risks.

Blockchain analytics can help explain where value appears to have moved. Travel Rule solutions can help transmit required originator and beneficiary information. Digital identity tools may improve customer identification. But none of these controls, on their own, fully identifies who the digital asset service provider behind the transaction is, nor describes its legal, regulatory and jurisdictional status.

This question is increasingly important. Treasury identifies risks relating to digital asset service providers, or DASPs, operating from jurisdictions with weak or non-existent AML/CFT obligations. Corporate structures spanning multiple jurisdictions, firms claiming to be regulated when they may only be incorporated, businesses that may serve U.S. customers while claiming not to be subject to U.S. obligations, and the use of services obscuring location all introduce opacity into who the DASP is.

For banks, payment firms, stablecoin issuers, DASPs and other regulated financial institutions, effective digital asset risk management requires a reliable way to identify, verify and monitor digital asset counterparties. This includes understanding the legal entity behind a brand or trading name, the countries in which it may have a legal footprint, the regulator(s) responsible

for supervision, permissions held, jurisdictions in which the service provider appears to operate, and any gaps between claimed and verified regulatory status.

Travel Rule compliance starts with understanding the counterparty

This is particularly acute in Travel Rule compliance. The Travel Rule is often treated as a data transmission requirement. But before an institution sends, receives or relies on Travel Rule information, it needs to understand the counterparty institution.

A firm should be able to ask:

- Who am I sending my customers' personally identifiable information (PII) to?
- What entity is behind this service?
- Is it regulated, where is it regulated, and is its regulatory status relevant to the service being provided?

On-chain analytics and off-chain intelligence are complementary controls

On-chain analytics is a necessary and valuable control, but it is not a substitute for off-chain counterparty intelligence.

A blockchain alert may identify exposure to an address, cluster, exchange, bridge, mixer, marketplace or other service. The next question is often whether that service is operated by a regulated DASP, an offshore VASP, an unregulated entity, a group affiliate, a prohibited business, or a firm claiming a status that cannot be independently verified.

The strongest digital asset financial crime control environment will therefore require a combined model, leveraging the capabilities of on-chain analytics, Travel Rule controls, digital identity and auditable off-chain DASP due diligence.

Off-chain due diligence as a control layer

VASPnet's work focuses on this off-chain due diligence layer.

VASPnet collects, structures, maintains and shares regulatory and publicly available reference data on digital asset service providers globally. This includes legal entity information, trading names, regulator-published status, source links, jurisdictional footprint, group relationships and affiliated entities, warning indicators, activity indicators and change history.

The purpose is to help obliged entities unambiguously and universally identify and evidence who they are dealing with in the digital asset ecosystem.

Counterparty DASP due diligence addresses five gaps in current controls

1. Brand-level claims of regulation are insufficient

A digital asset business may use multiple trading names, legal entities, affiliates and other associated entities. A registration in one jurisdiction may not apply to the contracting entity, the customer relationship, the relevant product or the jurisdiction into which services are being offered.

2. Jurisdictional arbitrage is difficult to assess without structured reference data

A DASP may be incorporated in one country, registered in another, operationally managed from a third and serve customers in many more. Such a global footprint is made more complicated with groups of entities trading under a single name.

We explored this issue further in our earlier commentary paper, "[Registered somewhere, active everywhere: what the FATF's oVASP report means for compliance teams.](#)"

Understanding this footprint is essential to assessing the risks identified by Treasury.

3. Effective controls must be examiner-ready

Institutions need to demonstrate not only that they reached a risk-based decision, but how they reached it. That requires source-linked evidence, timestamps, regulator references, search history, refresh records, decision logs and a clear rationale for the outcome.

4. Information sharing gaps remain a barrier

Treasury's report recognises the need for stronger mechanisms to share illicit finance insights and indicators across the financial sector. A structured, permissioned and auditable counterparty intelligence layer could help verified participants share relevant observations relating to digital asset counterparties, subject to appropriate legal, confidentiality and governance controls.

5. Policy language varies by regime

International standards refer to VASPs. The GENIUS Act uses DASP. The EU's Markets in Crypto-assets Regulation (MiCA) uses CASP. U.S. rules may also classify certain digital asset businesses as MSBs or other financial institutions.

Regulated firms and supervisors need a practical way to map these categories to real-world entities and services. Innovation also means modernising traditional controls.

Treasury's report is right to focus on innovation, and innovation can extend beyond analytics, AI or identity tools. It can also mean making traditional financial crime controls more effective, more auditable and better adapted to the digital asset ecosystem.

VASPnet would welcome further dialogue with Treasury, FinCEN and other relevant agencies on how counterparty DASP due diligence can complement blockchain analytics, Travel Rule compliance, digital identity and information-sharing initiatives.

Learn more

About VASPnet

VASPnet is the world's most assured source of regulatory data on virtual asset service providers (VASPs). Our VASPdata and VASPindex products give public and private sector entities the information they need to make well-informed, risk-based decisions on the VASPs they do business with.

To find out more, visit vaspnet.com and follow us on [LinkedIn](#).

Contact us at contact@vaspnet.com.

Author

Neil Samtani

24 June 2026

Copyright © 2026 Enhanced Compliance Solutions Inc.

All rights reserved.

VASPnet® is a registered trademark of Enhanced Compliance Solutions Inc.

VASPdata is a trademark of Enhanced Compliance Solutions Inc,

This article is for informational purposes only and is not legal or financial advice. The content is based on various sources and should not be used for making legal or financial decisions. Reader reliance on this information is at their own risk.