

CipherTrace Geographic Risk Report: VASP KYC by Jurisdiction



CipherTrace Cryptocurrency Intelligence
October 2020

This report was reproduced with permission from CipherTrace. The analysis and conclusions are CipherTrace's alone, and NICE Actimize had no editorial control over report contents.

About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance. Learn more at niceactimize.com

About CipherTrace

CipherTrace enables the blockchain economy by protecting cryptocurrency companies and financial institutions from security and compliance risks. Years of research have gone into developing the world's most complete and accurate cryptocurrency intelligence and forensics, covering more than 800 currencies. This visibility into the blockchain and virtual asset businesses helps protect banks and exchanges from cryptocurrency laundering risks, while protecting user privacy. CipherTrace also works with government agencies to bridge the gaps between regulation and the world of cryptocurrencies and blockchain.

CipherTrace is a founding member of TRISA, the leading open source industry standard to meet the Travel Rule requirement for secure information sharing while protecting cryptocurrency user privacy. TRISA enables cryptocurrency companies to comply with the Financial Action Task Force regulations that will shape the world of cryptocurrencies and bring them to institutional prominence as investment and cross-border payment technologies. Learn about the open source Travel Rule Information Sharing Architecture at trisa.io.

Executive Summary	4
The Importance of Strong KYC Processes	7
FATF Red Flag Indicators Related to Geographical Risks for Virtual Assets	7
KYC Regional Overview	8
56% of VASPs globally have weak or porous KYC	8
US, UK and Russia Host the Most VASPs with Weak KYC	9
Seychelles a Potential Money Laundering Heaven	10
Lack of KYC at Decentralized Exchanges Increases Money Laundering Risks	10
VASPs Without a Clearly Defined Domiciled Country	12
Appendix A: Methodology	14

Executive Summary

Effective Know-Your-Customer (KYC) protocols are a vital part of any anti-money laundering (AML) regime. When done right, KYC processes can help financial institutions better understand and manage their risks and prevent money laundering. However, it's one thing to have strong KYC guidelines on paper and another to implement them. By analyzing and probing the Know Your Customer (KYC) processes of over 800 VASPs in over 80 countries, CipherTrace geographically located where weak and porous KYC could be exploited by money launderers, criminals, and extremists.

56% of VASPs globally have weak or porous KYC

Despite existing crypto AML regulations, many countries continue to host virtual asset service providers (VASPs) with deficient KYC. CipherTrace research has discovered that in 2020, 56% of VASPs globally have weak or porous KYC processes, meaning money launderers can use these VASPs to deposit or withdrawal their ill-gotten funds with very minimal to no KYC. The more porous VASPs that allow deposits and withdrawals up to a specified dollar amount with little to no KYC risk encountering conventional money laundering tricks, like structuring to fly under the radar.

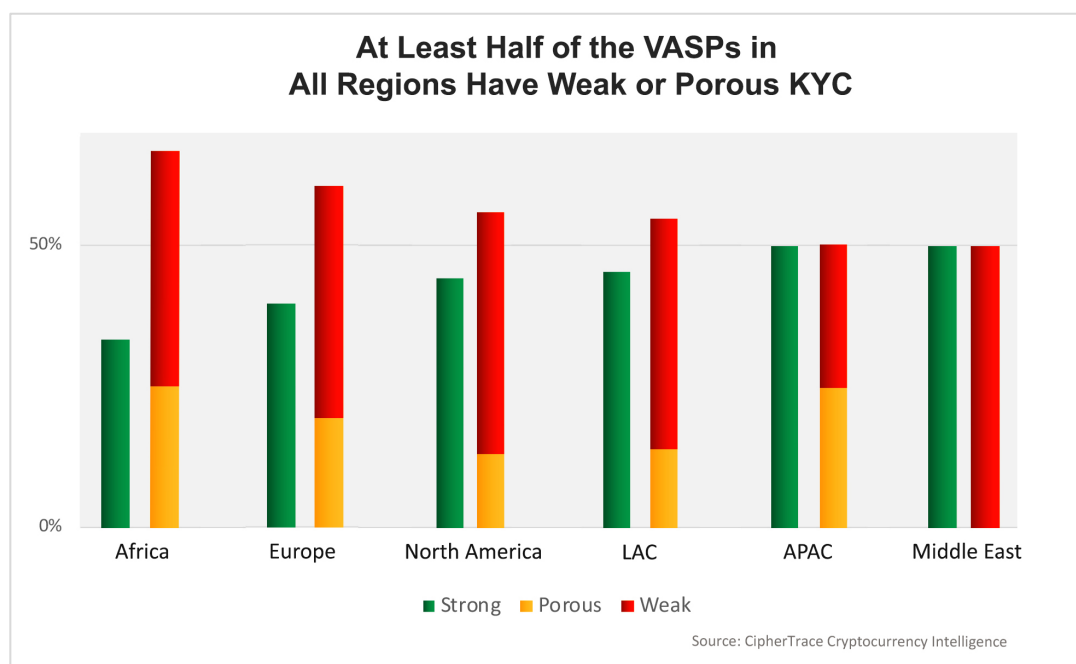


Figure 1

Notwithstanding the 5th Anti-Money Laundering Directive (AMLD5), CipherTrace researchers have discovered that Europe has the highest count of VASPs with deficient KYC procedures. Sixty percent of European VASPs have weak or porous KYC.

US, Singapore, and UK Host the Most VASPs with KYC Deficiencies


The US, Singapore, and the UK lead as the countries with the highest number of VASPs with weak or porous KYC. Although these regions host a higher volume of VASPs in general, the large count of VASPs in these countries that require little to no KYC demonstrates the ease and volume of potential offramps for money launderers.

When looking at the weakest KYC countries in the world, CipherTrace analysts discovered that 60% of the top 10 worst KYC countries in the world are in Europe, 20% are in Latin American and Caribbean countries, and the final 20% are in APAC countries.

DeFi Permissionless Transaction Volume Creates Regulatory Risks

The USD value locked in DeFi has grown exponentially in 2020, reaching 16 billion USD. Couple this growth with the fact that DeFi protocols are designed to be permissionless—meaning anyone in any country is able to access them without any regulatory compliance—and it's clear that DeFi has the potential to become a haven for money launderers.

While the operations of these exchanges are decentralized, the scale of their governance decentralization varies greatly. CipherTrace researchers found that over 90% of DEXs with a clearly domiciled country had deficient KYC, with 81% having little to no KYC whatsoever. According to some regulators, this lack of KYC may be a compliance violation, despite their decentralized nature.



“[DeFi Projects] are likely subject to various laws already, including securities law, potentially banking and lending laws—definitely AML/CTF laws.”

-Valerie Szczepanik, SEC

“We’ve seen [DeFi] projects that have been subject to vulnerabilities, attacks, hacks, manipulation,” said SEC Crypto Czar Valerie Szczepanik at the Parallel Summit on September 18, 2020. “We’ve seen structures that purport to enable users to lend money, earn interest, borrow money, exchange, take positions; these are all financial activities and they are likely subject to various laws already, including securities law, potentially banking and lending laws—definitely AML/CTF laws.”

Three-Quarters of African-Domiciled VASPs with Weak or Porous KYC are Domiciled in the Seychelles

72% of African-Domiciled VASPs are registered in the Seychelles and, 70% of those Seychelles-domiciled VASPs have bad or porous KYC. Fully 75% of all of Africa's KYC deficient VASPs, then, are domiciled in the Seychelles, making the small island country a boon for potential money launderers. Further analysis shows that a majority of the customer base for Seychelles-domiciled VASPs are foreign users, highlighting their money laundering potential.

Average VASP KYC Scores by Country

The average KYC levels in this report have been mapped in figure 1 below, with red representing poor KYC, yellow representing porous KYC, and green representing strong KYC. See Appendix A for the methodology used to grade VASP KYC Scores.

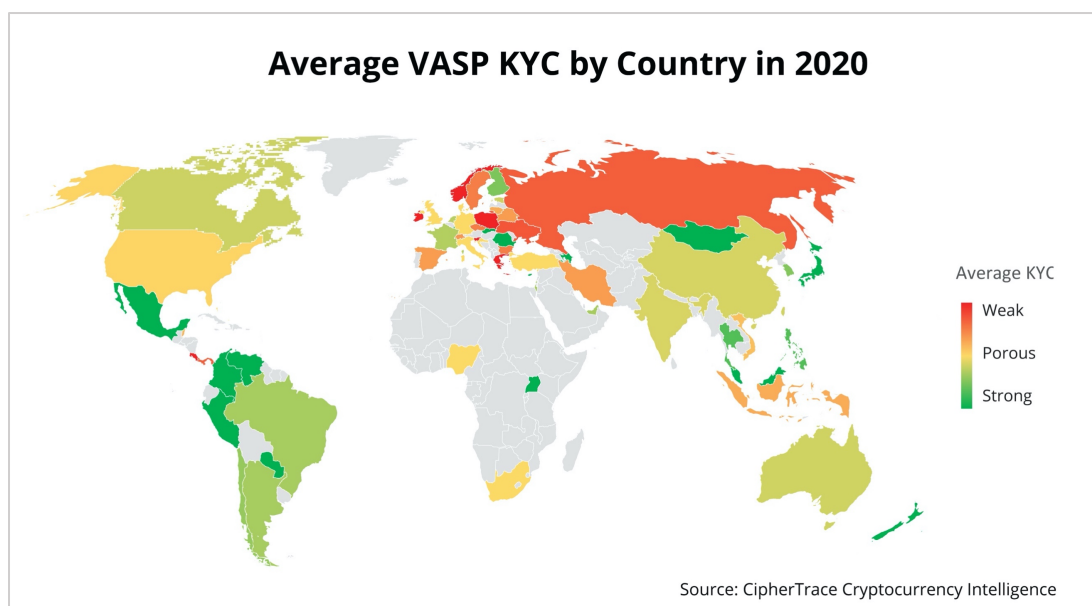


Figure 2

While this report gives valuable insight on the crypto money-laundering potential of a given country, KYC is only one factor when evaluating a VASP's overall risk. CipherTrace's attribution team analyzes KYC and transaction risks on over 800 VASPs. By integrating attribution data from active intelligence gathering, public and private intelligence sources, and open-source intelligence (OSINT), CipherTrace maintains the industry's most accurate pool of attribution data. This data ensures financial institutions have an accurate view of the KYC and transactional risk of a VASP.

The Importance of Strong KYC Processes

Financial Institutions employ Know Your Customer (KYC) processes to confirm the identity of their customer. These processes typically involve the collection and verification of a customer's personally identifiable information (PII)—including, but not limited to, government-issued ID, phone number, email address, physical address, and more. Exact KYC requirements vary by jurisdiction, meaning criminals can use jurisdictional arbitrage to choose geos with lax KYC procedures to further obfuscate their flow of funds.

Strong KYC procedures can mitigate money laundering. A VASP with strong KYC will know the real identities of users complicit in transactions involving stolen or nefariously gained cryptocurrency. Strong KYC procedures should also prevent bad actors from registering with fake credentials, such as synthetic IDs or stolen identities, making the laundering of cryptocurrency much harder. Weak KYC procedures, on the other hand, can easily lead to a VASP becoming a go-to location for criminals either to convert ill-gotten cryptocurrencies into fiat or to use the VASP as a mixing service, allowing criminals to convert coins and sever ties to previous flows of funds.

FATF Red Flag Indicators Related to Geographical Risks for Virtual Assets

In September 2020, FATF released their Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing Report. The report warns that criminals, when moving their illicit funds, “have taken advantage of the varying stages of implementation by jurisdictions on the revised FATF Standards on VAs and VASPs.” This action is known as jurisdictional arbitrage.

Criminals reportedly exploit the gaps in AML/CFT regimes by moving illicit funds to VASPs domiciled in jurisdictions with non-existent or minimal AML/CFT regulations on VAs and VASPs.

According to the FATF, VASPs should be wary of the following red flags involving KYC:

- Customers utilizing VASPs in a high-risk jurisdiction lacking, or known to have inadequate, AML/CFT regulations for VA entities, **“including inadequate CDD or KYC measures”**
- Customers receiving funds from or sending funds to VASPs **“whose CDD or KYC processes are demonstrably weak or non-existent”**

CipherTrace Armada helps VASPs detect these red flags by highlighting a sending or receiving VASPs KYC score to identify payments with VASPs that have **demonstrably weak or non-existent CDD and KYC** processes. Additionally, banks can use Armada to determine the KYC scores of the VASPs with which their customers are interacting.

KYC Regional Overview

56% of VASPs globally have weak or porous KYC

Despite existing crypto anti-money laundering (AML) regulations, many countries continue to host virtual asset service providers (VASPs) with weak or porous KYC. CipherTrace research has discovered that in 2020, 56% of VASPs globally have weak or porous KYC.

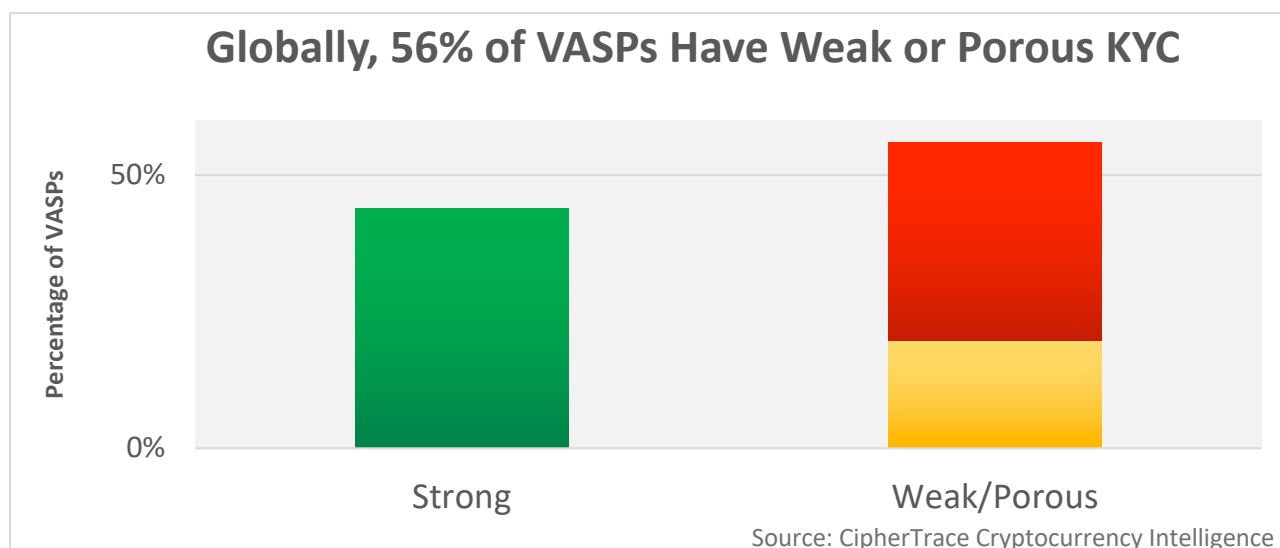


Figure 3

While these findings are an improvement from last year, when CipherTrace researchers found that two-thirds—about 65%— of the 120 most popular cryptocurrency exchanges had weak or porous KYC practices, it is clear that VASPs still have a long way to go when it comes to compliance. The high percentage of KYC-deficient VASPs make it easy for criminals to exploit these institutions and launder their funds.

For example, on March 2, 2020, two Chinese nationals—Tian Yinyin and Li Jiadong—were sanctioned by the US Office of Foreign Assets Control (OFAC) for their involvement in laundering stolen virtual currency from a 2018 crypto exchange hack perpetrated by the Lazarus Group. These funds were primarily laundered through VASPs by circumventing their KYC procedures. Notably, attempts to circumvent KYC practices at some VASPs failed after red flags led the VASPs to request a video conference with the account holder to verify his identity. The account holder refused, preventing him from using the VASP to launder funds.

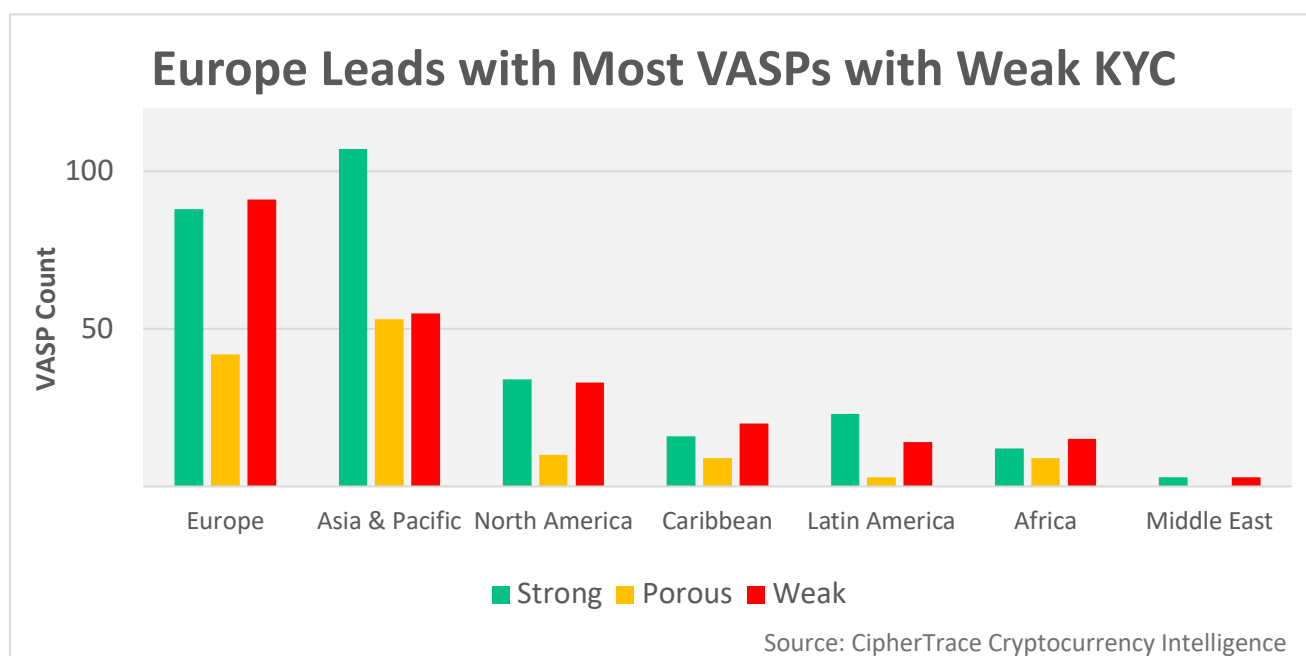


Figure 4

Figure 4 highlights the symmetry between strong and weak VASPs in different regions. While Europe leads with the most VASPs with weak KYC, the number two spot is an outlier. Despite being the region with the second highest count of weak KYC VASPs, APAC also leads as the region with the largest count of VASPs with strong KYC, as well as the region with the lowest percentage of weak and porous VASPs.

US, UK and Russia Host the Most VASPs with Weak KYC

The US, UK, and Russia lead as countries with the highest count of VASPs with weak KYC—meaning VASPs with major deficiencies in their KYC process that allow any daily deposit or withdrawal with very minimal to no KYC. Although there remains a higher volume of VASPs in this region in general, the large count of VASPs with such deficient KYC practices in these countries demonstrates the higher number of entry points for potential money launderers. While only 44% of US and 40% of UK exchanges were found to have weak KYC practices, these KYC deficiencies characterize 80% of Russian exchanges.

When looking at the countries with the highest count of combined weak and porous VASPs, the US, Singapore, and UK take the lead. The next two closest countries with large numbers of KYC-deficient VASPs are China and Russia, yet these two countries have between 31-44% fewer VASPs with weak or porous KYC than any of the three leading countries. Despite the US, Singapore and the UK having the largest count of weak and porous KYC VASPs in the world, their KYC averages are all still in the porous range, balanced by the equally large count of strong-KYC VASPs.

Seychelles a Potential Money Laundering Heaven

72% of African-Domiciled VASPs are registered in the Seychelles. 70% of Seychelles-domiciled VASPs have bad or porous KYC, totaling 75% of all of Africa's KYC-deficient VASPs, and thereby making the small island country a boon for potential money launderers. Further analysis shows that a majority of the customer base for Seychelles-domiciled VASPs are foreign users, highlighting the nation's money laundering potential. While the Seychelles' Anti-Money Laundering Act 2017 sought to bring more regulation into the country, most VASPs simply "maintain the right" to verify a user's identity for the purposes of complying, without ever actualizing that right. The new AML/CFT Act 2020 and Beneficial Ownership (BO) Act 2020 seek to rectify these deficiencies.

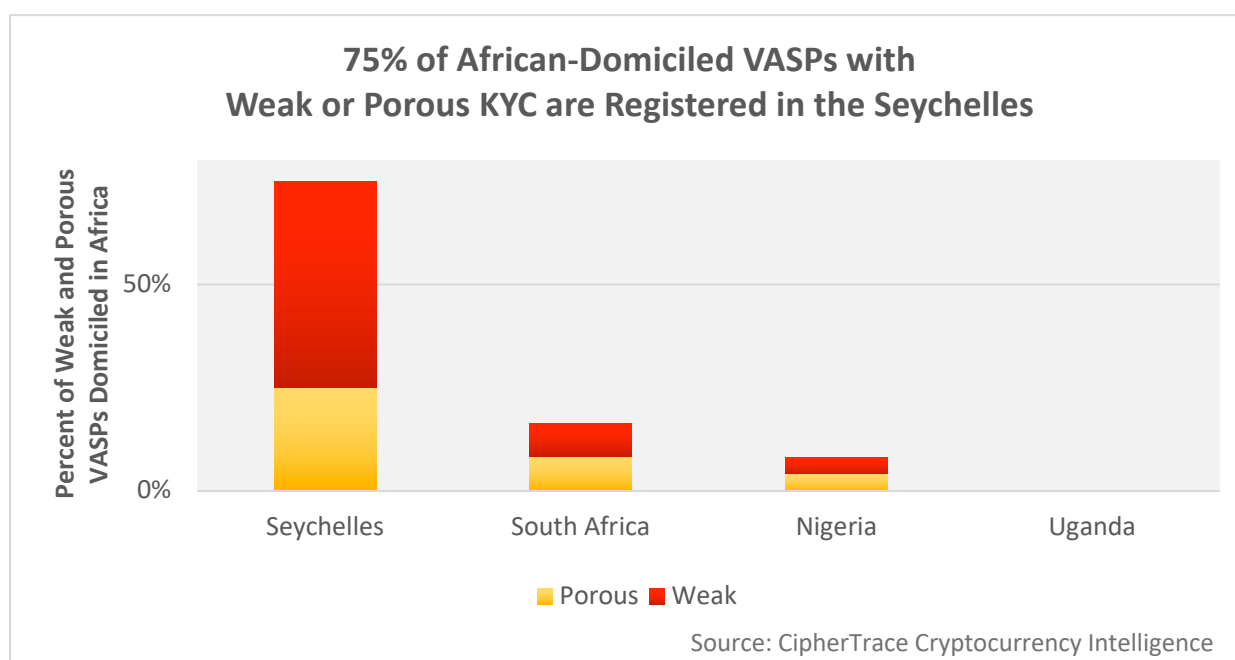


Figure 5

Lack of KYC at Decentralized Exchanges Increases Money Laundering Risks

Decentralized Finance (DeFi) is smart contract-based finance. The financial products, service, and instruments are implemented in code and made up of independent parts that are brought together without the use of traditional intermediaries like banks. DeFi structures are financial in nature and take on the functions and characteristics of regulated activities including operating as a broker dealer, lending funds, earning interest, and offering securities.

The USD value locked in DeFi has grown exponentially in 2020, thus creating potential new money laundering risks. According to CoinGecko, DeFi has locked up 37%—\$15.7 billion USD—of Ethereum’s total market capitalization. Because DeFi protocols are permissionless by design, they often lack any clear regulatory compliance. Anyone in any country can access DeFi with little to no KYC information collected. As a result, DeFi can easily become a haven for money launderers.

A Decentralized Exchange (DEX) is a type of cryptocurrency exchange that operates in a decentralized manner and enables peer-to-peer crypto trading. Because DEX’s are a type of DeFi application, they typically lack any KYC process. While the operations of Decentralized exchanges are decentralized, the scale of the governance decentralization varies greatly some operators are anonymous while other have offices, corporate structures and venture capital funding. For instance, Uniswap—located in San Francisco—has received venture investment capital from Andreessen Horowitz and Union Square Ventures. Yet, despite being US-domiciled, UniSwap benefits from the lack of regulatory clarity covering decentralized exchanges.

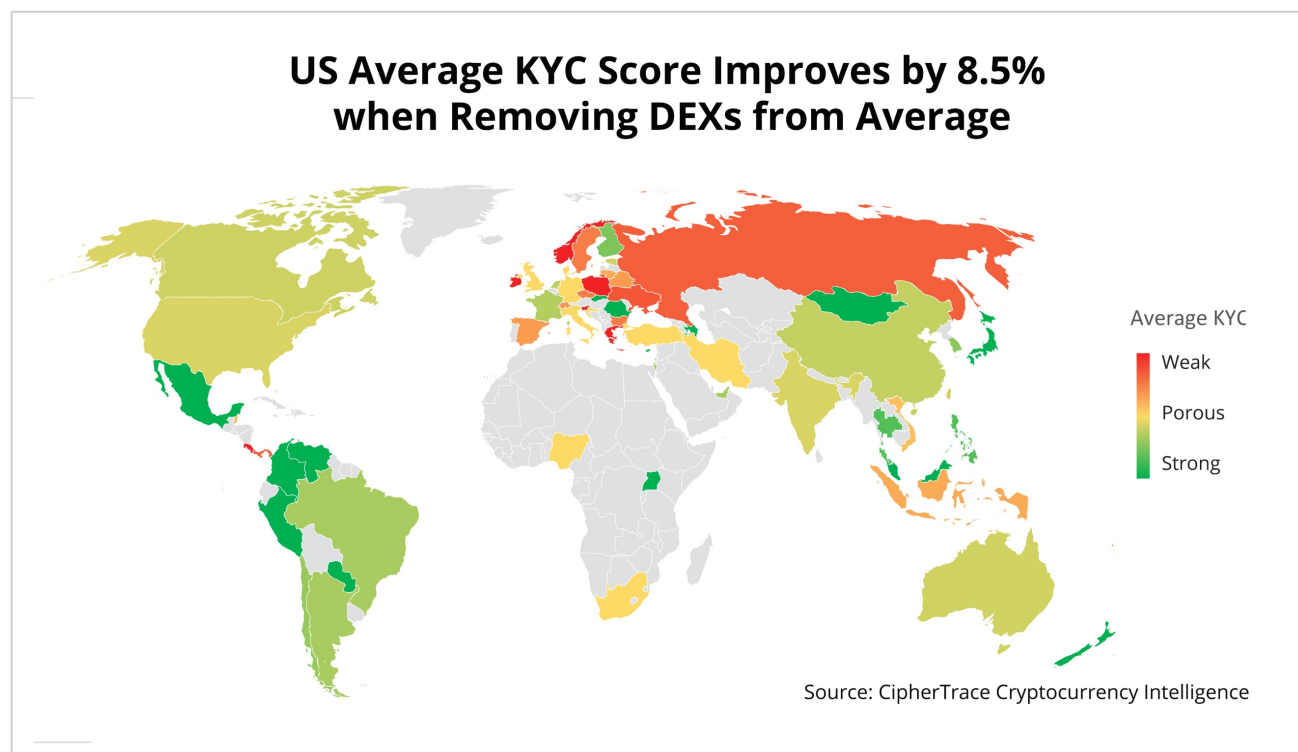


Figure 6

Because they have operated outside of regulatory supervision, it is no surprise that many DEXs have poor KYC scores. CipherTrace researchers found that over 90% of DEXs with a clearly domiciled country had deficient KYC, with 81% having little to no KYC whatsoever.

When we removed the DEXs that had clearly domiciled countries from our data, CipherTrace researchers found several countries had improved scores. Most notably, the United States KYC score improved by 8.5%, moving its average from porous (yellow) to strong-leaning (green).

Despite the decentralized nature and attributes of DEXs, regulators are beginning to pay closer attention to DeFi and their various regulatory obligations and money laundering potential. Funds stolen in the KuCoin hack on September 26, 2020 were quickly moved into DEXs such as UniSwap, prompting Dovey Wan of Primitive Ventures to tweet “All Defi infra are natural mixers with ultra low slippage.”



“All DeFi Infra are natural mixers with ultra low slippage”

-Dovey Wan, Primitive Ventures

As DeFi continues to grow, it’s plausible that these decentralized exchanges can fall under the scope of global regulators. FATF already considers decentralized exchanges “VASPs,” and FinCEN applies the same regulatory consideration to DEXs that it does to Bitcoin ATMs (BATMs). In the EU, the Markets in Crypto-assets Regulation (MiCA) Directive introduced on September 24, 2020 will impact DeFi projects that engage with EU citizens. According to XReg Consulting “There can be little doubt MiCA will present significant challenges for those involved in DeFi projects.”

Of the 51 DEXs CipherTrace analyzed, only 21 had countries of domicile.

VASPs Without a Clearly Defined Domiciled Country

CipherTrace has found that 85% of VASPs without a clear domiciled country have weak or porous KYC. These are VASPs that do not publicly release the country they are registered in on their website or in their terms and conditions or other documentation.

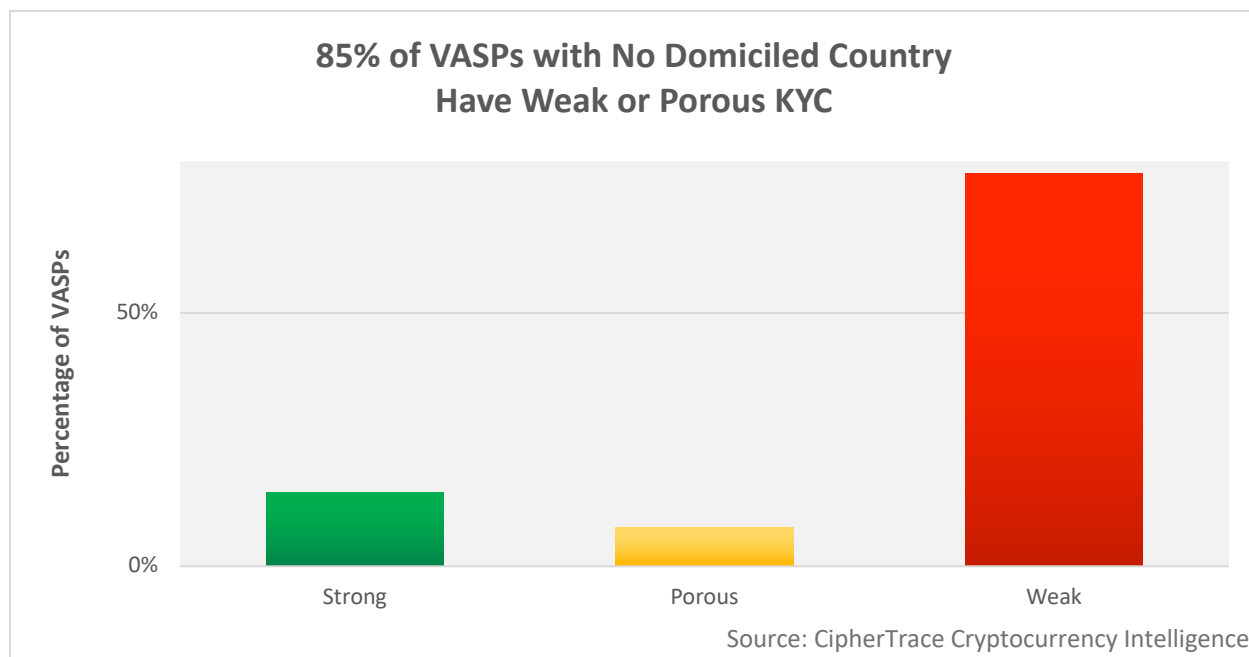


Figure 7

Many of these VASPs hide their jurisdictions to avoid having to register or comply with specific AML regulations, despite clearly serving customers in a given country. For example, despite a VASP having its website in Russian, promoting the exchange of rubles to bitcoin, and having access to several Russian banks, CipherTrace researchers were unable to find any legal connections to clearly label the VASP as domiciled in Russia. This included looking into the VASP's terms of service, as well as researching its "doing business as" (DBA) and checking Russian business directories.

The fact that these VASPs lean heavily on having little to no KYC highlights their intention to circumvent AML regulations. The lack of a clear domicile should be considered an AML red flag, especially when coupled with a poor KYC score.

Appendix A: Methodology

The CipherTrace Attribution Team tests all VASPs using a standardized criterion and rates them as “Weak,” “Porous,” or “Strong” based on how easy it would be to launder money after opening an account. The criteria are as follows:

- **Weak (Red)** – These exchanges have major deficiencies in their KYC process and allow any daily deposit or withdrawal with very minimal to no KYC: usually just an email address, name, and perhaps a phone number.
- **Porous (Yellow)** – These exchanges have minor weaknesses in their KYC process and allow deposits and withdrawals up to a specified dollar amount with little to no KYC. These practices are risky because common tricks, like structuring, can allow money laundering to fly under the radar. However, larger amounts may require a strong level of KYC.
- **Strong (Green)** – These exchanges require a very strenuous KYC process, requiring several steps to complete before users are able to make a deposit or withdrawal. They require an ID verification process and proof of address. Some require a phone call or video chat to complete the KYC process.

To determine the average KYC scores of each country and subsequent region, CipherTrace analysts assigned each VASP a 1 (strong), 2 (porous) or 3 (weak) to represent their respective KYC score.

While some VASPs may support many countries and regions, each VASP is assigned one country based on where that VASP is domiciled—not where their customers are located. Larger VASPs, such as Binance, may have multiple arms domiciled in different jurisdictions. Each of these arms is treated as a separate entity, with its own respective domicile, when applicable.

Domicile countries play an important role in the specific anti-money laundering (AML) regulations with which a VASP must comply. For example, to avoid uncertainty around its operational legality in the US, in 2019 Binance stopped providing services to US persons on its Global site. Instead, Binance launched Binance.US, domiciled in the United States, to comply with US-specific AML requirements.

Follow this code to read all of CipherTrace's quarterly reporting and learn more.



<https://ciphertrace.com/resources/>

CipherTrace protects financial institutions from cryptocurrency laundering risks and helps grow the blockchain economy by making it safe for consumers, trusted by investors and, accepted by governments.

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators.

Editorial Board, **Pamela Clegg and Dave Jevans**

Editor-in-Chief, **John Jefferies**

Financial Crime and Compliance Analyst, **Julio Barragan**