GeoComply

March 3rd, 2023

Crypto Policy Unit
Financial System Division
Treasury
Langton Cres
Parkes ACT 2600

Re: Token Mapping Consultation Paper, Request for Comment

Dear Director

On behalf of GeoComply, thank you for the opportunity to comment in response to the Department of the Treasury's Token Mapping Consultation Paper. We appreciate the Treasury's willingness to garner input from the public and industry stakeholders to address both opportunities and risks in the cryptocurrency ecosystem.

Founded in 2011, GeoComply provides fraud prevention and cybersecurity solutions that detect location fraud and help verify a user's true digital identity. GeoComply's solutions incorporate location, device, and identity intelligence with advanced machine learning to detect and flag fraudulent activity. The company's software is installed on over 400 million devices worldwide and processes over 1 billion monthly transactions, placing GeoComply in a unique position to identify and counter both current and newly emerging fraud threats.

This comment letter will address questions raised under Section A of the consultation paper, specifically the questions about the government's role in crypto regulation and the need for developing effective safeguards. This letter will also address the risks tokenization poses to existing AML/CTF regulations and sanctions laws.

200 Massachusetts Ave NW
Washington, DC, USA
20003

GeoComply.com
solutions@GeoComply.com

GeoComply

Role of Government:

The crypto ecosystem has seen unprecedented technological adoption and advancement in the last few years. Undoubtedly, the pandemic has accelerated the need for digital financial products. Although this technological evolution has created positive impacts, it has also created accessible entry points for global cybercriminals and bad actors looking to exploit financial systems from anywhere in the world. Just as technology innovates and evolves, so do the tactics and attacks of cybercriminals.

In light of this increasing sophistication, the Treasury must work collaboratively with other relevant government departments to establish comprehensive standards to safeguard the crypto sector from fraud, money laundering, and terrorist financing. While illicit use of cryptocurrency remains relatively small, with transactions involving illicit addresses representing 0.15% of cryptocurrency transaction volumes in 2021, this percentage still reflects billions of dollars of transactions.[1] As the crypto ecosystem develops into a mature pillar of the Australian financial system, these percentages of illicit activity may become increasingly threatening should they go unaddressed.

Safeguarding the crypto ecosystem from illicit exploitation will require enhanced customer due diligence and ongoing transaction monitoring. The rise of location-obfuscating technology threatens traditional financial intelligence techniques. Virtual Private Networks (VPNs), proxies, and other advanced location obfuscating technology enable users to hide their true location and access any platform from anywhere in the world. This allows illicit actors to anonymize their true digital identity and conduct nefarious activities ranging from money laundering to fraud. Naturally, mitigating such activities aligns with the government's priority “to keep our community safe from people who seek to do us harm.” [2]

---

[1] Chainalysis Team. 2022. Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity. *Chainalysis*
[2] Australian Government Department of Home Affairs. 2022. National Security.

GeoComply

Along with the Australian Transaction Reports and Analysis Centre (AUSTRAC) and the Australian Sanctions Office (ASO), the Treasury is in an optimal position to advance this priority, with regard to digital assets and the wider financial services industry.

Geolocation Safeguards:

One of the key factors enabling cybercriminals to perpetrate crimes is their ability to manipulate or conceal their true location. Manipulating or hiding their true location is a bad actor's first line of defense, making it a clear red flag. Faking location anonymizes identity and hides intention.

For this reason, detecting accurate geolocation information has been codified as a key pillar of financial law enforcement. For example, in its Guidance on Digital Identity, the Financial Action Task Force (FATF) states:

> *"Digital ID authentication for authorising account access may enable regulated entities to capture additional information, such as **geolocation**, IP address, or the identity of the digital device used to conduct transactions. This information can help regulated entities develop a more detailed understanding of the client's behaviour as a basis for determining when its financial transactions appear to be unusual or suspicious, and may assist law enforcement in investigating crimes."*[3]

However, as location obfuscating tools have become ubiquitous, determining a user's true location has become increasingly difficult. For example, it is estimated that nearly a third of all Internet users use a VPN .[4] Although there are legitimate reasons to use a VPN, they also enable users to manipulate their IP Address, and obfuscate - or "spoof" - their location. This type of behavior is a common denominator of online fraud.

[3]Financial Action Task Force. 2020. Financial Action Task Force's Guidance on Digital Identity
[4] Pijus Jauniskis, 2022. VPN statistics: Users, markets, & legality. *SurfShark, Cybersecurity and Internet Security.*

GeoComply

VPN usage puts companies operating in the crypto and financial services ecosystem at risk of non-compliance, especially with regard to jurisdictional regulations. Moreover, location obfuscation via VPNs and other more advanced tools, such as DNS proxies and Tor exit nodes that manipulate an IP address, have been successful in bypassing compliance programs due to the financial industry's reliance on IP Addresses to verify a user's location. To put it into perspective, IP address technology, first deployed in 1983, is over 40 years old.[5] Twenty-five years after the invention of the IP Address, Apple released the iPhone 3G with GPS chips. Despite the availability of GPS geolocation data, a more accurate and reliable form of geolocation, the majority of the financial industry still relies on IP addresses for anti-fraud and compliance.

Relying on IP address technology for fraud and compliance provides cybercriminals with the opportunity to leverage sophisticated and readily available location-obfuscating tools to access crypto platforms with minimal friction and scrutiny, exposing companies and consumers to risk. The continual proliferation of location spoofing technology means that monitoring IP addresses alone will limit institutions' ability to ensure compliance and maximize due diligence.

The highly anonymized nature of the crypto ecosystem demands more robust safeguards. A true risk profile and robust digital identity should incorporate multi-source geolocation data, including GPS information, Wi-Fi triangulation, GSM (cellular) data, and IP address monitoring, in addition to the detection of advanced location spoofing technologies.[6] Employing solutions that operate in the full breadth of the available data sources ensures that non-compliant persons and territories are obstructed from engaging with the Australian financial system.

In summary, incorporating comprehensive multi-source geolocation data (GPS, WiFi Triangulation, and GSM data) into compliance programs yield numerous positive effects, such as

[5] Internet Assigned Numbers Authority (IANA). 2022. Number Resources. *Overview.*
[6] Ibid

GeoComply

i. Facilitating more robust and reliable Know Your Customer (KYC) and Customer Due Diligence (CDD) processes to authenticate identity;

ii. Ensuring that suspicious activity can be monitored and prevented in real-time (for example, account location jumping, signaling account takeover);

iii. Creating an audit trail for improved reporting and traceability of all transactions;

iv. Supporting law enforcement and creating efficiencies in investigations;

v. Effectively geofencing FATF high-risk countries and sanctioned jurisdictions; and

Vi. Enhancing Anti-Money Laundering (AML)/Counter Financing of Terrorism (CFT)/Proliferation Financing (PF) compliance.

Conclusion

As fintech and digital assets continue to globalize, so too will cybercriminals – and their ever-advancing techniques. The innovation of fraud prevention and compliance must race ahead of cybercriminal innovation, supported by bodies such as Treasury, AUSTRAC, and ASO, as financial institutions develop and implement compliance programs as sophisticated as the malicious actors in this space.

Multi-source geolocation data is a valuable part of authentication that helps digital identity verification, consumer authentication, and compliance by accurately determining the end user's location. It is a non-biased, privacy-preserving strategy to ensure compliance and fraud prevention by verifying the identity of end users. Geolocation and location spoofing detection are essential parts of creating a transparent and safe internet and digital economy for all.

GeoComply

Thank you for the Treasury's long-standing commitment to ensuring a secure financial system. We look forward to continued collaboration on these critical issues.

200 Massachusetts Ave NW
Washington, DC, USA
20003

GeoComply.com
solutions@GeoComply.com