GEOCOMPLY

8/26/2021

Committee Secretary
Senate Legal and Constitutional Affairs Committee
Department of the Senate
PO Box 6100
Parliament House
CANBERRA ACT 2600
AUSTRALIA
Via email: seniorclerk.committees.sen@aph.gov.au

To Whom It May Concern,

RE: GeoComply response to the Senate Legal and Constitutional Affairs Committee Consultation on the Adequacy and Efficacy of Australia's Anti-money Laundering and Counter-terrorism Financing (AML/CTF) Regime

On behalf of GeoComply, thank you for the opportunity to provide information and comment on Australia's AML/CFT Regime.

We appreciate the willingness of the Senate Legal and Constitutional Affairs Committee (hereinafter, 'the Committee') to solicit information from industry and other stakeholders to ensure Australia's AML/CFT regime is adequate and efficient, to further our shared goal of protecting the integrity of the Australian financial system.

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 along with advanced machine learning to detect and flag fraudulent activity. By integrating GeoComply's solutions into their processes and risk engines, organizations are able to identify

1750-999 West Hastings Street
Vancouver, BC
V6C 2W2

GeoComply.com
solutions@GeoComply.com
+1 604.336.0877

GEOCOMPLY

fraud earlier in a user's engagement, better establish their true digital identity and empower digital trust.

The company's software is installed on over 400 million devices worldwide and analyzes over 3 billion transactions a year, placing GeoComply in a unique position to identify and counter both current and newly emerging fraud threats.

While money laundering and terrorist financing are complex, one solution is already in place today to address risk, and enhance trust and transparency in financial ecosystems. Geolocation data, a frequently under-utilized tool in the fight against fraud, is already a 'known' quantity in its ability to flag suspicious activity.

However, Internet Protocol (IP) geolocation (hereinafter, 'Geo-IP'), which dates back to the 1990s, is still the principal geolocation check in the financial services industry today, despite a) how easy it is to spoof or manipulate, and b) the wealth of stronger and more reliable geolocation data points that are available on most devices in the world today.

By way of this comment letter, GeoComply addresses the following terms of reference posted by the Committee:

> b. The extent to which Australia's AML/CTF regulatory arrangements could be strengthened to:
>
> i. address governance and risk-management weaknesses within designated services, and
>
> ii. identify weaknesses before systemic or large-scale AML/CTF breaches occur;
>
> e. Australia's compliance with the Financial Action Task Force (FATF) recommendations and the Commonwealth Government's response to applicable recommendations in applicable FATF reports.

GeoComply outlines that risk and compliance management frameworks relying upon Geo-IP fall short of identifying, measuring, monitoring and controlling risks

GEOCOMPLY

associated with money laundering and terrorist financing. In line with FATF recommendations, there is a better way to address such risks; namely, leveraging authentic, multi-sourced geolocation data (such as GPS, WiFi Triangulation, GSM and Geo-IP) to strengthen customer due diligence (CDD) and monitoring. Such technology and data ensure that suspicious activity can be detected in real-time and enhances the reportable data available to regulators and law enforcement for investigative purposes.

I. Geolocation Introduction

The field of digital identity is experiencing significant developments. Such recent developments include the FATF offering a comprehensive illustration of the role that device-based geolocation data can play within the realm of CDD in multiple reports, including:

- Guidance on Digital Identity[1];
- Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers[2];
- Guidance on Proliferation Financing Risk Assessment and Mitigation[3];
- Opportunities and Challenges of New Technologies for AML/CFT[4].

There are numerous benefits to utilizing geolocation data and spoofing detection solutions, such as:

[1] Financial Action Task Force's Guidance on Digital Identity (March 2020), page 13, 22, 31, 64: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf

[2] Financial Action Task Force's Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (June 2019), page 41: https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

[3] Financial Action Task Force's Guidance on Proliferation Financing Risk Assessment and Mitigation (June 2021), page 39: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf

[4] Financial Action Task Force's Opportunities and Challenges of New Technologies for AML/CFT (July 2021), page 29: https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf

GEOCOMPLY

a) Facilitating more robust and reliable Know Your Customer (KYC) and CDD processes;
b) Ensuring that suspicious activity can be monitored and prevented in real-time;
c) Creating an audit trail for improved reporting and traceability of all transactions;
d) Effectively geofencing high-risk and sanctioned nations; and
e) Enhancing Anti-Money Laundering (AML)/Counter Financing of Terrorism (CFT)/Proliferation Financing (PF) compliance.

Despite the FATF's leadership in this area, the majority of financial institutions (FIs) are not leveraging the benefits available from this highly accurate and reliable location data for security or risk management purposes.

In light of the scale of the threat associated with those that exploit digital assets for nefarious purposes, the advantages of leveraging the value within authentic geolocation data for CDD are worth emphasizing.

II. The extent to which Australia's AML/CTF regulatory arrangements could be strengthened to address governance and risk-management weaknesses within designated services.

Within Australia's Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1), made under section 229 of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006, reportable details for suspicious matters involving digital currencies includes the Internet Protocol (IP) address information of the first person, if known.

Geo-IP has traditionally been relied upon by FIs as an indicator of location within risk management and CDD frameworks. However, risk and compliance management frameworks that rely upon Geo-IP for location intelligence fail to address the risks associated with online transactions.

GEOCOMPLY

Relying upon an IP address alone for geolocation is associated with the following vulnerabilities:

- Spoofing and anonymising of IP addresses is extremely commonplace[5];
- There is no real correlation between a user's physical location and their mobile IP address[6]; and
- IP geolocation is rarely accurate to within a half of a mile.

Approximately one-third of internet users rely on a Virtual Private Network (VPN).[7] There are an extensive range of tools available to anonymise identity online, including VPNs, proxies, Tor, Fake Location Apps, GPS anonymisers, emulators, rooted or jailbroken devices, among others.

The increasing ability of consumers to operate anonymously on the internet creates significant challenges to trust in online transactions, including:

- Facilitating uninterrupted online criminal activities and allowing customers to operate while evading detections by law enforcement;
- Masking real IP addresses and preventing device tracking, which lowers the quality of data available for reporting and to ensure the integrity of transactions;
- Enabling users to bypass geographic restrictions and conduct transactions from high-risk or sanctioned regions; and
- Obfuscating reporting and oversight capabilities.

---

[5] Global Web Index, VPN Users Around the World (Q4, 2018): https://www.globalwebindex.com/hubfs/Downloads/VPN_Usage_Around_The_World.pdf?utm_campaign=VPN%20users%20around%20the%20world%202019&utm_medium=email&_hsmi=72644829&_hsenc=p2ANqtz--utuiaCfTSPX5uq5UvBG4hjEhVX-vecr-bYcqm0kvuVOjF-fxjB3MEMTJFdcf_aAT9n2mcqxs2I_RjDVoazoA4WIbPhA&utm_content=72644829&utm_source=hs_automation

[6] NixIntel, Geolocating Mobile Phones With An IP (July 5, 2020): https://nixintel.info/osint/geolocating-mobile-phones-with-an-ip/

[7] Global Web Index, VPN Users Around the World (Q4, 2018): https://www.globalwebindex.com/hubfs/Downloads/VPN_Usage_Around_The_World.pdf?utm_campaign=VPN%20users%20around%20the%20world%202019&utm_medium=email&_hsmi=72644829&_hsenc=p2ANqtz--utuiaCfTSPX5uq5UvBG4hjEhVX-vecr-bYcqm0kvuVOjF-fxjB3MEMTJFdcf_aAT9n2mcqxs2I_RjDVoazoA4WIbPhA&utm_content=72644829&utm_source=hs_automation

GEOCOMPLY

Based on our experience operating globally in the anti-fraud and geolocation space for over a decade, we know that a tool to anonymise location is frequently the first line of defense for an actor engaging in nefarious activity online.

To address the risks posed by the proliferation of anonymising and spoofing tools, certain institutions have started checking IP addresses against lists of VPNs, Tor exit points, and other non-trusted IP Addresses, blocking any matches[8]. While these measures are a step in the right direction in reducing risk, there is a better way to provide actionable location intelligence for security and risk management purposes; leveraging multi-sourced geolocation data. This is critical to addressing the risks associated with digital assets by ensuring that CDD is robust, reliable and protected from exploitation.

Therefore, Australia's AML/CTF regulatory arrangements could be strengthened to address governance and risk-management weaknesses. By including geolocation data within designated services, reportable compelling evidence can be identified for suspicious matters involving digital currencies.

III. The extent to which Australia's AML/CTF regulatory arrangements could be strengthened to identify weaknesses before systemic or large-scale AML/CTF breaches occur.

By incorporating geolocation data into reportable details for suspicious matters involving digital currencies, FIs strengthen their ability to detect suspicious activity in real-time, before large-scale AML/CFT breaches occur. Such accurate data strengthens a FI's ability to create a secure digital identity, in addition to their ability to evaluate risk and detect suspicious and fraudulent behaviour.

[8] Paul, Weiss, Rifkind, Wharton & Garrison LLP, Economic Sanctions and Anti-Money Laundering Developments: 2019 Year in Review (January 2020). Page 22, 37. Available here: https://www.paulweiss.com/media/3979308/31jan20-aml-year-in-review.pdf

GEOCOMPLY

In line with FATF recommendations, by collecting multiple authentication factors, an authentication process becomes more robust and trustworthy[9]. In addition, periodic geolocation authentication throughout the course of an online interaction can give a better understanding of consumer behaviour, facilitating the monitoring of anomalous or suspicious behavior.[10] For example, a user's latitude/longitude or IP-based location coordinates jumping a large distance in a short period of time can indicate account takeover.

Therefore, geolocation authentication at varying stages during an online session, combined with the power of real-time and historical risk analytics enables suspicious activity to be detected and flagged. Such controls go a long way in detecting and deterring illicit actors at an earlier stage.

With authentic geolocation data, FIs would have far more robust and effective risk management processes, by enabling early detection of suspicious activities and a holistic overview of real-time and historic behavioral patterns.

IV. Australia's compliance with the Financial Action Task Force (FATF) recommendations and the Commonwealth Government's response to applicable recommendations in applicable FATF reports.

As previously mentioned, the FATF offers a comprehensive illustration of the role that device-based geolocation data can play within the realm of CDD, AML and CFT in multiple reports.

For example, in its Guidance on Digital Identity, FATF states:

---

[9] Financial Action Task Force's Guidance on Digital Identity (March 2020): page 22. Available here: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf

[10] Financial Action Task Force's Guidance on Digital Identity (March 2020): page 64. Available here: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf

GEOCOMPLY

> *"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."*[11]

In addition, in its Guidance For a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (VASP), FATF states:

> *"VASPs are also encouraged to collect additional information to assist them in verifying the customer's identity when establishing the business relationship (i.e., at onboarding); authenticate the identity of customers for account access; help determine the customer's business and risk profile and conduct ongoing due diligence on the business relationship; and mitigate the ML/TF risks associated with the customer and the customer's financial activities. Such additional, non-core identity information, which some VASPs currently collect, could include, for example an IP address with an associated time stamp; geolocation data; device identifiers; VA wallet addresses; and transaction hashes."*[12]

Moreover, in its report entitled Opportunities and Challenges of New Technologies for AML/CFT, FATF states:

> *"Onboarding tools that allow for quick CDD and client traits analysis (such as geolocation, credit checks, anti-fraud software and others) would also enrich*

[11] Financial Action Task Force's Guidance on Digital Identity (March 2020), page 37: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf

[12] Financial Action Task Force's Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (June 2019), page 41: https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

GEOCOMPLY

> *the CDD and monitoring process and lead to a more accurate understanding of the nature of the business relationship, as well as its impact to the institutions."*[13]

Accordingly, certain countries have followed FATF recommendations pertaining to the collection of geolocation data to reduce AML/CFT risks. For example, the Mexican Ministry of Finance and Public Credit amended Article 115 of the law for credit institutions titled "Disposiciones"[14], obliging banks and other financial institutions to collect and conserve their clients' geolocation on their digital platforms with the goal of mitigating money laundering and fraud as well as combating the financing of terrorism.

In accordance with rules 4 Ter, 16 Bis and 24, the Ministry of Finance and Public Credit obliges credit institutions to obtain the geolocation of the devices when:

a. They open an account or celebrate a contract through non-face-to-face devices,
b. Integrate the user's identification file; or
c. Perform operations in a non-face-to-face way (via digital platforms).

In a press release, the Comisión Nacional Bancaria y de Valores (the National Banking and Securities Commission) states:

> *"This measure is derived from the international commitments adopted by Mexico as a member of the Financial Action Task Force (FATF). Each modification to the Provisions seeks to adapt to the international standards that said body has implemented to combat money laundering and terrorist financing, and which have been recognized by various countries, as well as by*

[13] Financial Action Task Force's Opportunities and Challenges of New Technologies for AML/CFT (July 2021), page 29: https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf

[14] Diario Oficial de la Federación (2021): https://www.dof.gob.mx/nota_detalle.php?codigo=5554909&fecha=22/03/2019

GEOCOMPLY

international organizations such as the World Bank and the Monetary Fund. International. In that sense, this obligation is in line with the Guide on Digital Identity released by the FATF in March 2020."[15]

Therefore, GeoComply respectfully recommends that the Committee incorporates FATF's recommendations pertaining to leveraging geolocation data to enhance AML/CTF frameworks by strengthening digital identity.

V. Final Remarks

GeoComply offers these recommendations with the aim to assist the Committee in its mission to ensure that individuals making digital transactions operate in a safe and sound manner, and comply with applicable laws and regulations. Thank you for the Committee's long-standing commitment to ensuring a secure and stable Australian financial system and we look forward to continued collaboration on these critical issues.

Sincerely,

David Briggs
CEO

[15] Comisión Nacional Bancaria y de Valores (March 2021): https://www.gob.mx/cnbv/articulos/inicia-la-implementacion-de-la-geolocalizacion-de-dispositivos-para-operaciones-financieras?idiom=es