GEOCOMPLY

7/9/2021

James P. Sheesley, Assistant Executive Secretary
Federal Deposit Insurance Corporation,
550 17th Street N.W.,
Washington, D.C. 20429.
Via email: comments@fdic.gov
Attention: Comments-RIN 3064- ZA25

Dear Mr. James P. Sheesley,

RE: Request for Information and Comment on Digital Assets (RIN 3064-ZA25)

On behalf of GeoComply, thank you for the opportunity to provide information and comment on digital assets.

We appreciate the willingness of the Federal Deposit Insurance Corporation's (FDIC) to solicit information from industry and other stakeholders to ensure those dealing with digital assets operate in a safe and sound manner, to further our shared goal of protecting the integrity of the United States (U.S.) 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 fraud earlier in a user's engagement, better establish their true digital identity and empower digital trust.

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

GeoComply.com
solutions@GeoComply.com
+1 604.336.0877

GEOCOMPLY

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 the risks associated with digital assets are complex, one solution is already in place today to address risk, and enhance trust and transparency in the digital asset ecosystem. 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 questions posted by the FDIC's Request For Information (RFI):

> 4. To what extent are IDIs' existing risk and compliance management frameworks designed to identify, measure, monitor, and control risks associated with the various digital asset use cases? Do some use cases more easily align with existing risk and compliance management frameworks compared to others? Do, or would, some use cases result in IDIs' developing entirely new or materially different risk and compliance management frameworks?
> 5. What unique or particular risks are challenging to measure, monitor, and control for the various digital asset use cases? What unique controls or processes are or could be implemented to address such risks?

GeoComply outlines that risk and compliance management frameworks relying upon Geo-IP fall short of identifying, measuring, monitoring and controlling risks associated with digital assets. There is a better way to address such risks; namely, leveraging authentic geolocation data to strengthen customer due diligence (CDD)

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

GeoComply.com
solutions@GeoComply.com
+1 604.336.0877

and monitoring. Such technology and data ensure that regulators and law enforcement are receiving the most accurate, highly useful and relevant data from industry for investigative purposes.

I. Geolocation Introduction

The field of digital identity is experiencing significant developments. Such recent developments include the Financial Action Task Force's (FATF) Guidance on Digital Identity[1] and Guidance For a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (VASP)[2], offering a comprehensive illustration of the role that device-based geolocation data can play within the realm of CDD.

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

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.

[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

GEOCOMPLY

The value of geolocation data and spoofing detection in CDD has already been realized by regulated institutions, subject to the Bank Secrecy Act, in the U.S. internet gaming (iGaming) and sports betting market.[3]

Despite the FATF's and U.S. iGaming industry's leadership in this area, the majority of insured depository institutions (IDIs) 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. Existing Risk and Compliance Management Frameworks' Ability to Identify, Measure, Monitor and Control Risks Associated with the Various Digital Asset Use Cases

Geo-IP has traditionally been relied upon by financial institutions 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, including but not limited to those that involve digital assets.

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

- Spoofing and anonymizing of IP addresses is extremely commonplace[4];

[3] Morgan Stanley's US Sports Betting & Online Gambling Primer 2.0 (June 2020): page 9. Available here: http://linkback.morganstanley.com/web/sendlink/webapp/f/bdpe7elk-3qlc-g000-98c1-005056015000?store=0&d=UwBSZXNlYXJjaF9NUwA3OTVjMDk5Mi1hYzRiLTExZWEtOTEwZC0yOWZhMmFjOTFjNTI%3D&user=7vrd7od50gbh9-56&__gda__=1844219955_77e34ed1d3af98375892f6322c32dbf6

[4] Global Web Index, VPN Users Around the World (Q4, 2018): https://www.globalwebindex.com/hubfs/Downloads/VPN_Usage_Around_The_World.pdf?utm_camp

GEOCOMPLY

- There is no real correlation between a user's physical location and their mobile IP address[5]; 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).[6] There are an extensive range of tools available to anonymize identity online, including VPNs, proxies, Tor, Fake Location Apps, GPS anonymizers, 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, lowering the quality of data available for reporting and to ensure the integrity of transactions;
- Enable users to bypass geographic restrictions and conduct transactions from high-risk or sanctioned regions; and
- Obfuscating reporting and oversight capabilities.

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

---

aign=VPN%20users%20around%20the%20world%202019&utm_medium=email&_hsmi=72644829&_hsenc=p2ANqtz--utuiaCfTSPX5uq5UvBG4hjEhVX-vecr-bYcqm0kvuVOjF-fxjB3MEMTJFdcf_aAT9n2mcqxs2I_RjDVoazoA4WlbPhA&utm_content=72644829&utm_source=hs_automation

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

[6] 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_RjDVoazoA4WlbPhA&utm_content=72644829&utm_source=hs_automation

GEOCOMPLY

To address the risks posed by the proliferation of anonymizing and spoofing tools, certain institutions have begun checking IP addresses against lists of VPNs, Tor exit points, and other non-trusted IP Addresses, blocking any matches[7]. 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 by authenticating 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.

III. Controls and Processes To Address Risks

Geolocation data collected from the device, such as GPS, WiFi Triangulation and GSM, enhances risk management and addresses certain risks posed by digital asset transactions. Multi-sourced geolocation data gives far more accurate intelligence into a user's true location, while providing some protection against spoofing[8]. Such accurate data strengthens an IDIs ability to create a secure digital identity, in addition to their ability to evaluate risk and detect suspicious and fraudulent behaviour.

For CDD, we respectfully suggest the following should be collected:

1. The genuine, device-based geolocation data (WiFi Triangulation, GPS, GSM) of the user at the point of transaction;

[7] 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

[8] The risk of spoofing cannot be eliminated. While there exist a number of tools to spoof an IP address, there also exists a number of tools to manipulate other types of geolocation data. Therefore, while it is true that adoption of additional data points into a multi-factor authentication process increases confidence in delivering sufficient authentication, such confidence could be misplaced unless practical steps are taken to eliminate the risk of simultaneously creating a new threat; data tampering and/or spoofing of each additional data point.

2. The genuine IP address of the user, authenticated by viable anti-spoofing software in real-time to detect anonymizing tools; and
3. A device identifier that captures a digital fingerprint of technology used to make a transaction.

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, IDIs 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. Final Remarks

GeoComply offers these recommendations with the aim to assist the FDIC in its mission to ensure that individuals transacting with digital assets operate in a safe and sound manner and comply with applicable laws and regulations. Thank you for

[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

the FDIC's long-standing commitment to ensuring a secure and stable U.S. financial system and we look forward to continued collaboration on these critical issues.

Sincerely,

David Briggs
CEO
david@geocomply.com