



July 13, 2020

Director Kenneth A. Blanco
Financial Crimes Enforcement Network
U.S. Department of the Treasury
P.O. Box 39
Vienna, Virginia 22183-0039

Via electronic submission: Docket Number FINCEN-2020-0004 and the specific Office of Management and Budget (OMB) control numbers 1506-0001, 1506-0006, 1506-0015, 1506-0019, 1506-0029, 1506-0061, and 1506-0065.

Dear Director Blanco:

Re: GeoGuard Response to FinCEN's Invitation to Comment on the Proposed Renewal of Currently Approved Information Collections Relating to Reports of Suspicious Transactions

On behalf of [GeoGuard](#), thank you for the opportunity to comment on the proposed renewal of currently approved information collections relating to reports of suspicious transactions.

We appreciate FinCEN's willingness to solicit feedback from industry and other stakeholders to ensure that the information collected in Suspicious Activity Reports (SARs) is "highly useful" and actionable intelligence to further our shared goal of protecting the integrity of the U.S. financial system.

At GeoGuard, we focus solely on geolocation-based security, fraud detection and the protection of digital content and assets. As the independently rated market leader for protection against VPNs and Proxies, we help a wide range of industries guard against fraud and piracy while ensuring geolocation compliance with minimal user friction. GeoGuard provides a suite of geolocation-based solutions that are combined with human intelligence in order to stop internet users from spoofing their location. Our software is installed in over 300 million devices worldwide, putting GeoGuard in a uniquely powerful position to identify and counter both the current and newly emerging geolocation fraud threats.

By way of this comment letter, we outline recommended solutions to strengthen the type of data that is collected as part of the SAR reporting process, with a particular focus on expanding geolocation data fields for cyber indicators, beyond the current standard of an IP address, to ensure that SARs truly reflect the most accurate, useful and relevant data.



IP Over-Reliance Creates Avoidable AML and CFT Deficiencies

While we commend the efforts of FinCEN in expanding the scope of SARs to include cyber indicators, such as IP addresses, based on our experience of operating globally in the geolocation space, we know that:

- Spoofing and anonymizing of IP addresses is extremely commonplace and indeed has been found to have happened in multiple cases that FinCen have investigated recently;
- The IP address of a mobile device using cellular data does not provide any geolocation insight and as such is just as effective a tool for bad actors as a VPN; and
- IP geolocation is rarely accurate to within a half of a mile.

However, there is a better way to help identify and investigate suspicious activity and it is already being embraced by the financial services industry.

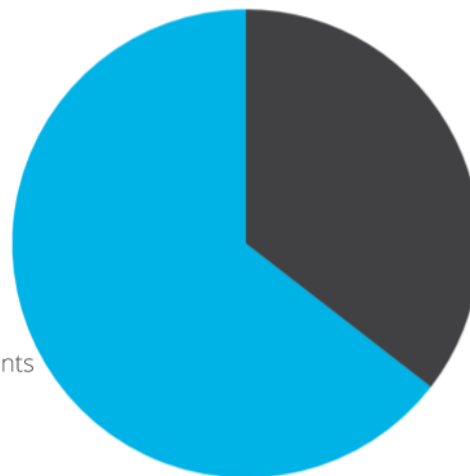
As illustrated in the below graph, 35% of the most commonly downloaded financial apps are asking for location.

■ **Asked for Access to Location?**

No

64.5%

| | |
|---------------|----------------------|
| Barclays | Acorns |
| BMO | E*TRADE |
| Capital One | Robinhood |
| HSBC | Binance US |
| Schwab Mobile | Bittrex |
| CashApp | Coinbase |
| Flywire | Chime |
| OFX | Credit Karma |
| PayPal | Simple |
| TransferWise | Fidelity Investments |



Yes

35.5%

Bank of America Mobile
Chase Mobile
DBS digibank SG
Discover Mobile
Wells Fargo Mobile
Citi mobile
MoneyGram
Western Union
Venmo
Zelle
Ally

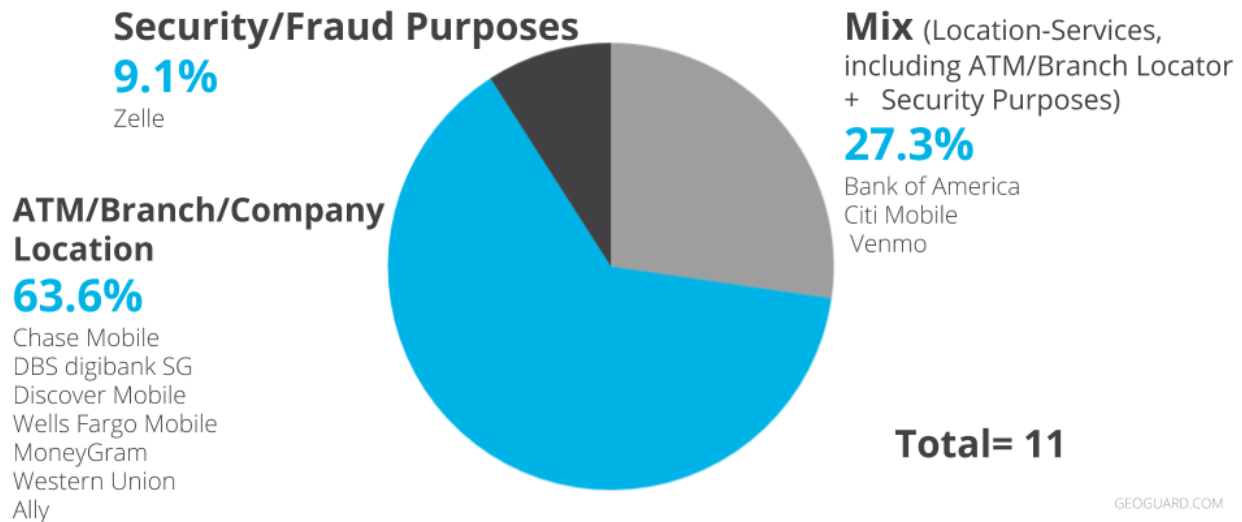
Total= 31

GEOGUARD.COM

However, currently nearly two thirds of the apps are NOT leveraging the benefits available from this highly accurate location data for compliance and/or security purposes, but instead for their own marketing/commercial objectives such as branch finders:



■ If **Yes**, what is the breakdown for primary reasons of location access?



In light of the size and scale of the cybersecurity threat facing the global financial industry today it seems as though the advantages of leveraging the value within this location data are well worth emphasizing.

IP address technology is 20 years old, and there is little in the digital ecosystem from those days that could still be considered “fit for purpose” in light of the advances since then in technology and cyberthreats.

An IP address is commonly and readily anonymized. If a core goal of fraudsters is to steal personally identifiable information to open up fraudulent accounts and conduct illicit activity, one of the first layers of protection they will utilize to mask their true identity is a tool to spoof their location. Therefore, if regulated financial institutions have neither the correct tools nor collect the correct data to determine if an IP address is fraudulent, they may report inaccurate and therefore meaningless information as part of their SAR reporting obligations.

The technology exists to determine whether geolocation data points, including IP addresses, have been spoofed. Such technologies go a long way in detecting and deterring illicit actors at an earlier stage and providing financial regulators and law enforcement with more reliable and useful data.

In addition, IP geolocation is rarely accurate. It commonly crosses state borders in the US and is redundant for mobile transactions. Device-based geolocation (i.e. WiFi



Triangulation, GPS, GSM) is far more precise and readily collected in alternative industries (for example, eCommerce).

Moreover, aggregating multiple geolocation data points, as opposed to a single authenticator, provides stronger protection against the spoofing. For example, discrepancies between the IP location and the device location data might indicate IP spoofing.

Distinguishing between multi-source geolocation data and an IP address is critical, as the use of accurate, authentic and unaltered geolocation data is essential to establishing a person's true digital identity and goes beyond what a simple (and easily spoofed) IP address can provide.

Authentic and Unaltered Geolocation Data: Mitigating AML and CFT Risks and Instilling Accuracy and Integrity

To fulfil the Bank Secrecy Act's (BSA) objective of collecting the most highly data and actionable intelligence, we respectfully suggest the following updates to the SAR reporting process:

To ensure that FinCEN and law enforcement are provided with more authentic, accurate and valuable BSA data, it is recommended that FinCEN includes additional cyber indicators on SARs for device-based geolocation data points such as GPS; GSM; and WiFi. Given the abundance of cyber events identified in recent SAR filings, the opportunity exists to drastically increase the volume of valuable and meaningful data submitted to FinCEN, aligned with efforts to foster a more effective and efficient BSA regime. In addition, such valuable data creates internal efficiencies and far more robust and effective risk management processes for the regulated financial sector, by enabling earlier detection of a potential bad actor's illicit activities. These changes are particularly important amid the [increasing cyber threats](#) currently faced by financial institutions amid the COVID-19 pandemic.

In addition, it is important that financial institutions are equipped with the correct tools and insights to determine whether the data points provided - for example, IP addresses - are indeed authentic and genuine. Otherwise, FinCEN and law enforcement are at risk of collecting and pursuing meaningless leads. As previously mentioned, technologies are readily available to determine whether an IP address has been spoofed. Moreover, aggregating multiple geolocation data points could indicate where spoofing may be occurring and would provide more accurate insight to the true location of the individual.


GeoGuard offers these recommendations with the aim to better fulfill the mission of the BSA; namely, government and law enforcement receiving the most highly useful



information for investigations and for financial crime detection and prevention to ensure the integrity of the U.S. financial system.

We thank you for FinCEN's long-standing commitment to setting regulatory policies that ensure a secure and stable U.S. financial system and we look forward to our continued collaboration on these critical issues.

Sincerely,

DocuSigned by:

349B960BA0BD4E1...

David Briggs
CEO

david@geoguard.com