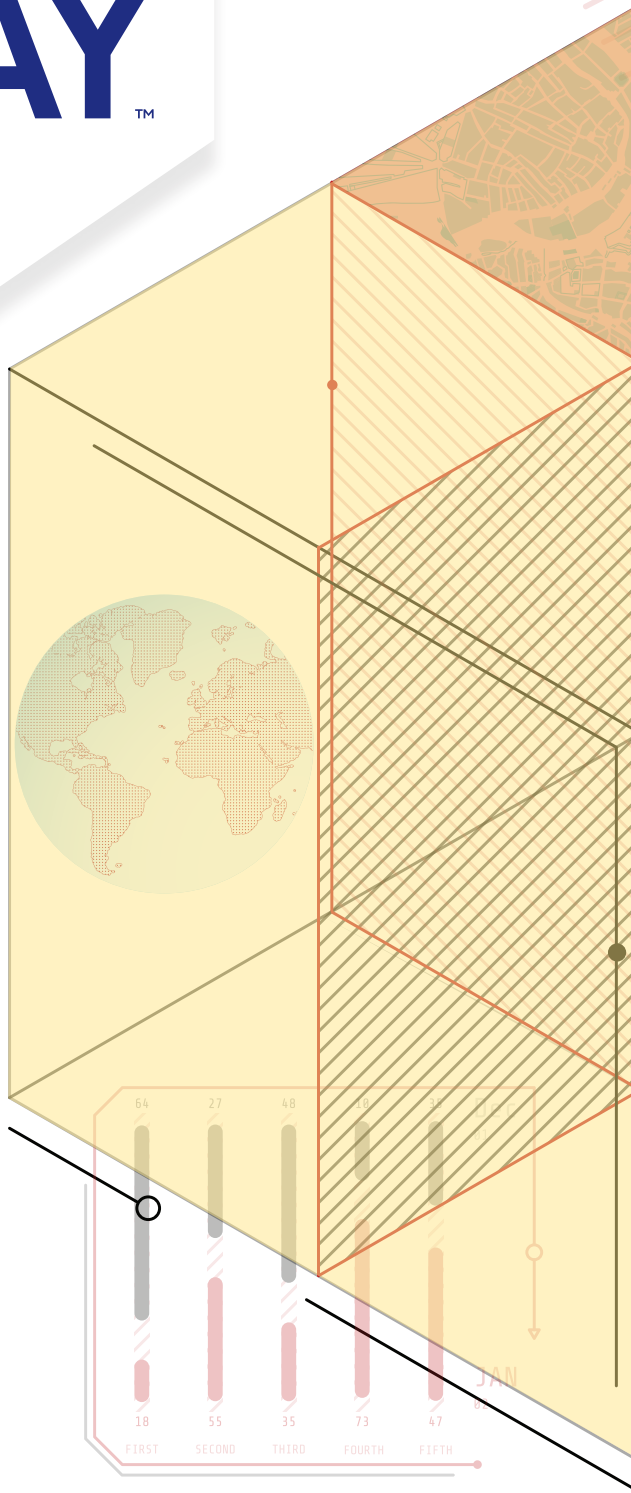
ACAMS TODAY™

# OFAC calls for geolocation tools and blockchain intelligence




The Office of Foreign Assets Control (OFAC) has focused on cryptocurrency over the last few years. OFAC has used sanctions and enforcement actions to go after those facilitating money laundering and sanctions evasion, sending a clear message to crypto businesses that sanctions compliance is a foundational infrastructure.

But how can a cryptocurrency business ensure that it is not engaging with a sanctioned individual or a sanctioned entity? How does an exchange know that a customer is located in Iran, North Korea, Sudan or another sanctioned jurisdiction? What does OFAC expect when it comes to crypto sanctions compliance?

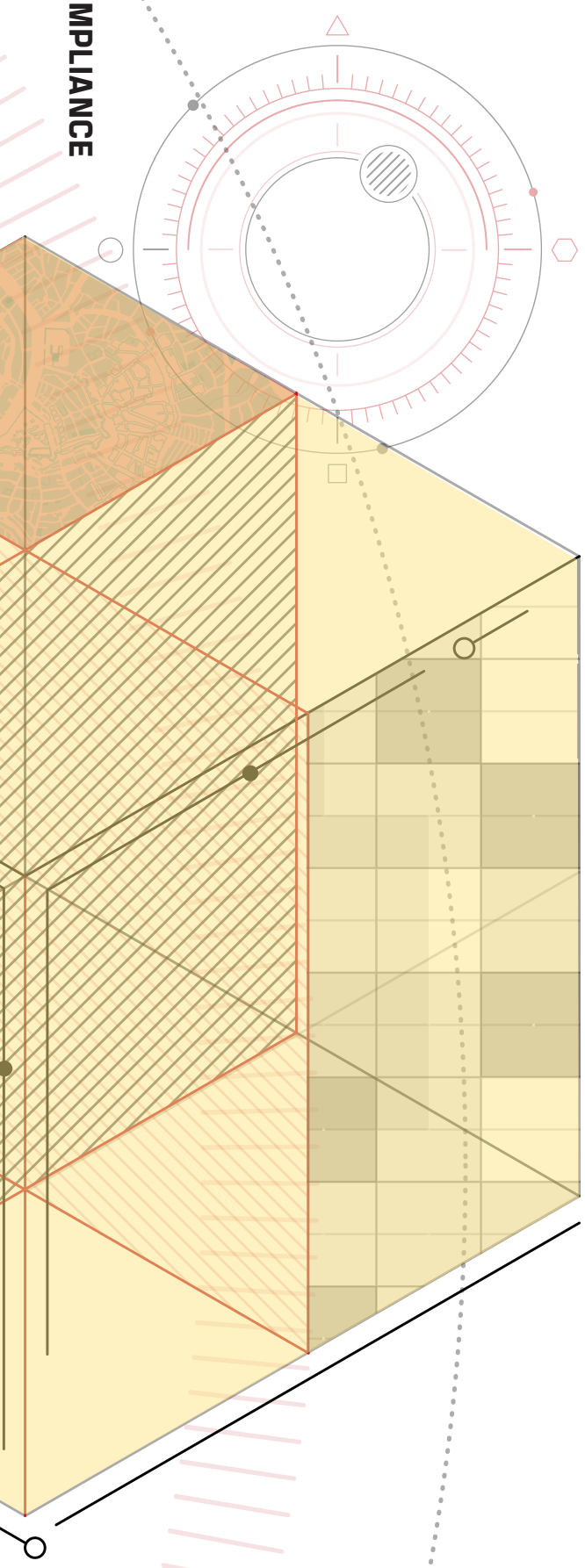
Spoiler alert: OFAC expects robust compliance to include geolocation and blockchain intelligence tools to mitigate the risk of sanctions exposure.

TRM

GeoComply

ACAMS

Reprinted with permission from the September–November 2022, Vol. 21 No. 4 issue of *ACAMS Today* magazine, a publication of ACAMS



## OFAC's guidance to cryptocurrency businesses

In October 2021, OFAC published the "Sanctions Compliance Guidance for the Virtual Currency Industry,"[1] which outlines how OFAC sanctions guidance applies to the cryptocurrency space in the same way it does for traditional financial institutions (FIs). The October 2021 guidance also provides digestible guidance for FIs and cryptocurrency businesses on best practices to combat the use of virtual currency by sanctioned persons or jurisdictions.

OFAC's Associate Director of Compliance and Enforcement Lawrence Scheinert explained how the agency is thinking about crypto sanctions compliance on TRM Talks, "The growing prevalence of virtual currency as a payment method brings greater exposure to sanctions risks—like the risk that a sanctioned person or a person in a jurisdiction subject to sanctions might be involved in a virtual currency transaction."[2]

He added, "Accordingly, the virtual currency industry—including technology companies, exchangers, administrators, miners, wallet providers, and users—play an increasingly critical role in preventing sanctioned persons from exploiting virtual currencies to evade sanctions and undermine U.S. foreign policy and national security interests."[3]

The guidance highlights several key areas, including the use of geolocation tools to prevent IP addresses that originate in sanctioned jurisdictions. It also highlights the need to employ monitoring and investigations software that can identify transactions involving cryptocurrency addresses associated with sanctioned individuals and entities listed on the specially designated nationals (SDN) list.

## The importance of geolocation tools

In its October 2021 guidance, OFAC explained, "Virtual currency companies with strong sanctions compliance programs should be able to use geolocation tools to identify and prevent IP addresses that originate in sanctioned jurisdictions from accessing a company's website and services for [an] activity that is prohibited by OFAC's regulations."[4]

According to OFAC Director Andrea Gacki, the agency has also "been highlighting the importance of using geolocation tools as an effective internal control both in our sanctions compliance guidance for the virtual currency industry … but also through our enforcement actions."[5]

One example is OFAC's enforcement action against payment processor BitPay,[6] which agreed to pay over $500,000 for violations of multiple sanctions programs. The U.S. Department of the Treasury explained that BitPay allowed people who appear to have been located in the Crimea region of Ukraine, as well as Cuba, North Korea, Iran, Sudan and Syria, to transact with merchants in the U.S. and elsewhere using digital currency on BitPay's platform—even though BitPay had location information, including IP addresses and other data about the location of these people prior to effecting the transactions.

The U.S. Department of the Treasury has made clear that it expects cryptocurrency businesses to use tools such as those from GeoComply[7] to block users in high-risk or sanctioned jurisdictions. Cryptocurrency businesses do this through "geofencing," the practice of creating a virtual parameter around a real-world location using location data from a user's device. Device-based location data is accurate within meters, enabling cryptocurrency firms to "carve out" tightly linked geographic regions, such as the Crimea, Luhansk and Donetsk regions within the territory of Ukraine.

Sophisticated tools further strengthen geolocation compliance[8] by mitigating the risk of virtual private networks (VPNs), proxies and other anonymizers that manipulate IP addresses. These tools gather and authenticate geolocation data from multiple sources—such as IP addresses, Wi-Fi triangulation and GPS signals—to ensure a consumer is located in a legal jurisdiction and is not attempting to manipulate their location.

Cryptocurrency businesses can analyze this data to determine its source and potential association with malware, advanced spoofing tools such as virtual machines, anonymizers (VPNs, proxies and Tor exit nodes) and any links to high-risk jurisdictions and activity.

## The importance of blockchain intelligence

In addition to the use of geolocation, OFAC expects cryptocurrency businesses to utilize blockchain intelligence tools to monitor transactions and screen cryptocurrency wallets to check for sanctioned individuals or entities.

"Blockchain intelligence" is the practice of organizing and analyzing on-chain data—by the time stamp, currency, address or the service used to conduct the transaction. For example, to map trends or patterns of activity, detect links to off-chain data points or surface other attributes that might indicate risk. Blockchain intelligence layers the raw, accessible public blockchain data with threat intelligence.

Blockchain intelligence, also known as "blockchain analytics," allows law enforcement, regulators and compliance professionals more visibility over financial flows than they ever had before, in real time. The nature of blockchain—the open and distributed ledger upon which tokens can be sent—means that each transaction is verified and logged in a shared, immutable record, along with the time stamp of the transaction and the addresses involved. This data from the public blockchain is accessible to anyone on the blockchain.

For example, when OFAC adds a cryptocurrency address to its SDN list—perhaps associated with a sanctioned Russian, North Korea's Lazarus Group or a terrorist financier—that address is tagged in a blockchain intelligence tool as being connected to a sanctioned individual or entity. This allows a cryptocurrency exchange, for example, to flag any transactions involving that address, assess the risk and take any action that may be required based on regulatory requirements.

In addition, sanctions compliance professionals can use a blockchain intelligence tool to trace and track the movements of funds (to and from an address associated with the sanctioned address) to build an investigation.

## Conclusion

Over the last few years, we have seen OFAC focus on cryptocurrency, with sanctions designations against noncompliant exchanges and enforcement actions against crypto businesses that did not have the tools to screen for sanctioned individuals, entities and jurisdictions. Crypto compliance professionals are the tip of the spear when it comes to stopping illicit actors and mitigating sanctions risks for their businesses and the larger crypto economy. They need the right tools to comply with OFAC but, more importantly, to ensure that the crypto economy continues to flourish. AT

*Ari Redbord, head of legal and government affairs, TRM Labs, Washington, D.C., ari@trmlabs.com, Twitter: @ARedbord*

*Elizabeth Cronan, vice president, government relations, GeoComply, Washington, D.C., elizabeth.cronan@geocomply.com, LinkedIn*

1 "Sanctions Compliance Guidance for the Virtual Currency Industry," *Office of Foreign Assets Control*, October 2021, https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf

2 "Watch the Interview: Treasury Comments On Release of Ransomware-Related Data and Guidance," *TRM Labs*, October 15, 2021, https://www.trmlabs.com/post/watch-the-interview-treasury-comments-on-release-of-ransomware-related-data-and-guidance

3 Ibid.

4 "Sanctions Compliance Guidance for the Virtual Currency Industry," *Office of Foreign Assets Control*, October 2021, https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf

5 Andrea Gacki, Office of Foreign Assets Control director, *the ACAMS Sanctions Summit*, February, 3, 2022.

6 "OFAC Enters Into $507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions," *U.S. Department of the Treasury*, February 18, 2021, https://home.treasury.gov/system/files/126/20210218_bp.pdf

7 "Slash Regulatory Risk with Location Intelligence," *GeoComply*, https://www.geocomply.com/industries/financial-services/cryptocurrency/?utm_source=acamstoday.org&utm_medium=referral&utm_campaign=partnership&utm_content=blog

8 "How Virtual Currency Companies Can Raise the Compliance Bar," *GeoComply*, https://www.geocomply.com/how-virtual-currency-companies-can-raise-compliance-bar/?utm_source=acamstoday.org&utm_medium=referral&utm_campaign=partnership&utm_term=geolocation_compliance&utm_content=blog