

SPOTLIGHT ON SANCTIONS

Geolocation is More Than Just a Postal Code

A Spotlight on Geolocation and IP Address
Screening to Maintain Compliance with the
Office of Foreign Assets Control (OFAC)
Sanctions Programs

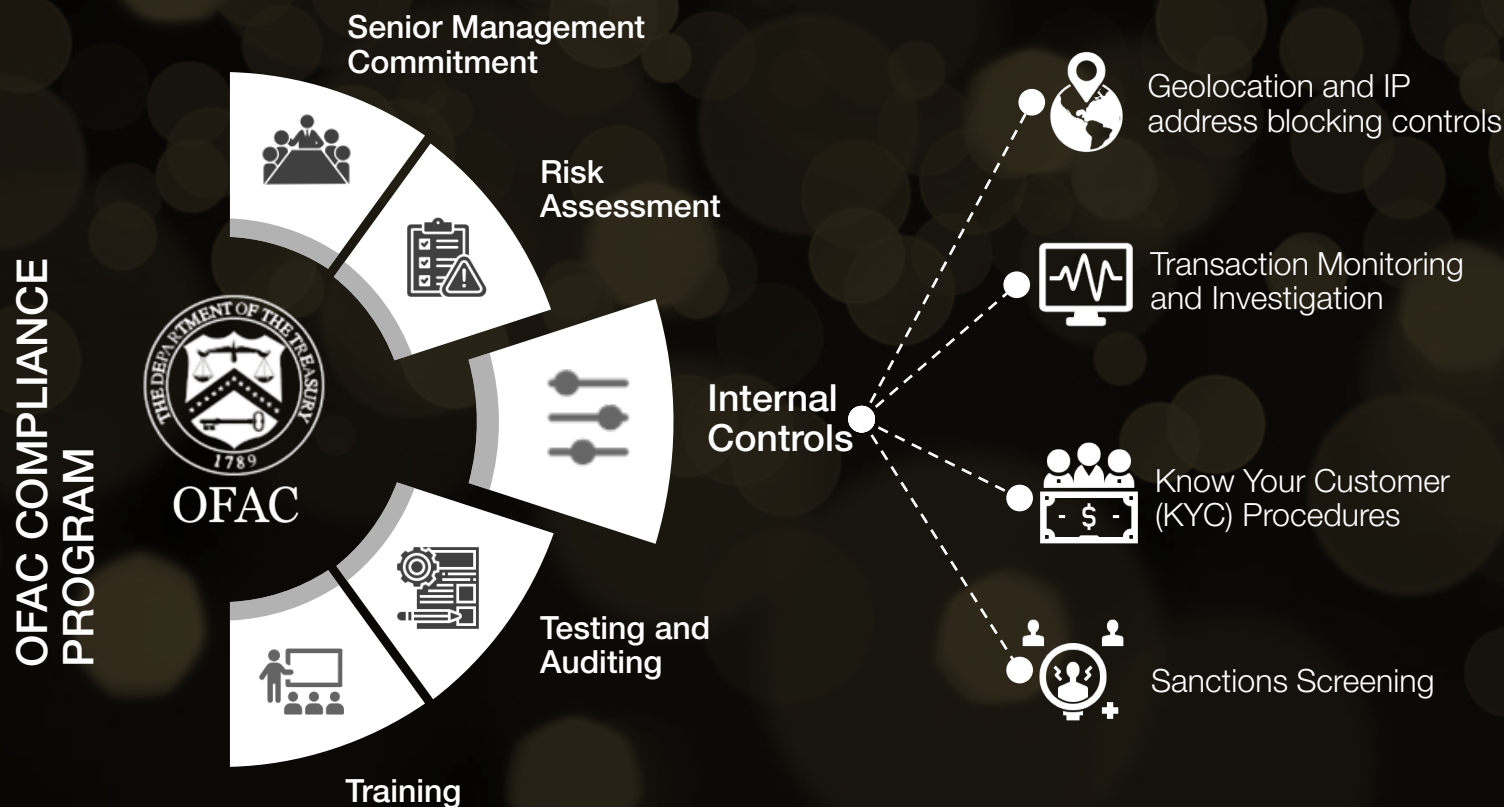


RISK | STRATEGY | CYBER COMPLIANCE MANAGEMENT



Implementing Geolocation to Maintain Sanctions Compliance

OFAC's October 2021 "Sanctions Compliance Guidance for the Virtual Currency Industry" recommends that sanctions compliance programs should include geolocation tools and Internet Protocol (IP) address-blocking as part of their internal controls. However, this guidance is not limited to virtual currency participants, rather when providing services globally, screening for location information through IP addresses and customer information to identify a potential sanctions nexus, is particularly important in mitigating the risk of providing services to individuals in jurisdictions subject to sanctions. In 2023, five (5) out of OFAC's seventeen (17) Enforcement Actions resulted in almost \$1B in civil monetary penalties, which highlights the lack of IP location screening as a key deficiency.





UNDERSTANDING GEOLOCATION

- Geolocation is the ability to track a device's whereabouts using Global Positioning System (GPS), cell phone towers, Wi-Fi access points, or a combination of these, such as smartphones, tablets, laptops, smartwatches, and fitness trackers.
- Device-based data collection relies on GPS or cellular networks. As long as the device has location-based services, a GPS chip, and a cellular network signal, an organization can access these services to find an individual general location. Server-based data collection is tied to an individual's device IP address. Regional internet registries manage and send out IP address information in specific regions worldwide.
- Combined data collection is the assembling of both device and server data. This method can return information that has been bypassed if an individual's IP address is routed through a virtual private network (VPN) or another proxy server.



GEOLOCATION ENABLING THE BUSINESS

- Geolocation is a powerful way for an organization to improve its marketing. An IP address can determine a customer's country, region, state, city, postal code, time zone, and exact coordinates. Organizations can analyze the customer base and make better business decisions based on the information.
- When an e-commerce site is in multiple countries and a customer lands on the organization's website, the website can cater to the individual by using the IP geolocation to take them to the site built specifically for that region—creating a tailored shopping experience.
- Fraud and security teams utilize the geolocation information to better detect fraudulent behavior on websites and mobile apps. If the location sharing is enabled on a device and it does not match the login/payment location, then the transaction can immediately be declined preventing loss to the organization and inconvenience to the customer.



MEETING GEOLOCATION OBLIGATIONS

- The organization may deploy a more enhanced due diligence and sanction screen at customer onboarding. For example, sanctioned countries can be screened by collecting the delivery and billing location. The organization can utilize this information in the sanctions screening process to prevent violations.
- Organizations can implement geofencing barriers on its website. Active geofences require an end user to opt-in to location services and a mobile app to be open. Passive geofences are always on; they rely on Wi-Fi and cellular data instead of GPS and work in the background. The geofence would detect and prevent access to the organization's website from restricted jurisdictions.
- Screening IP addresses against sanctioned jurisdictions when customers access, login, download software or mobile apps, or attempt to make a payment.



Discover
what
Stratis
Advisory
can do
for you



OFAC Sanctions Risk Assessment

Whether a financial institution, logistics company, import/export company, etc. understanding your exposure to OFAC sanctions programs and the quality of implemented risk mitigants is critical to maintaining compliance with OFAC. Stratis can execute your OFAC risk assessment to identify broader risk identification and control mitigation across your business operations.



Screening Vendor Due Diligence, Implementation, Testing, and Gap Analysis

Multiple vendors provide list screening services from limited to exhaustive lists. However, most of those vendors focus exclusively on name screening at onboarding and in transactions. Compliance with OFAC sanctions requires broader systems, inclusive of cybersecurity systems, to form a comprehensive screening program. Stratis can help you assess vendors, implement, tune, and test your new screening systems, and tune and gap existing systems to ensure appropriate coverage.



NYS DFS Part 504 Annual Transaction Monitoring and Watchlist Filtering Certification of Compliance

Operating as a New York State Department of Financial Services (NYS DFS) regulated institution such as a bank, insurance company, money transmitter, trust company, etc. (or applying for a license) requires an organization to annually certify to maintaining a compliant transaction monitoring (AML) and watchlist filtering (OFAC) program. Stratis can assess the readiness of your organization to submit a certification of compliance prior to the annual April deadline.





StratisAdvisory

LAUNCH | SCALE | OPTIMIZE