FRAUD-CHECKED ADVANCED GEOLOCATION FOR:

# MERCHANT ACQUIRERS

**350+** anti-fraud checks on every transaction

**4200+** fake location apps and VPN/Proxy checks

**100K+** unique fraudulent users blocked every month

GEOGUARD

Fraud Has No Place To Hide

The highly competitive nature of the PayFac industry means that merchant acquirers are continually streamlining their onboarding processes to improve merchant acquisition rates. However, reducing customer friction creates a trade off between convenience and risk.

## Frictionless onboarding exposes merchant acquirers to various risks:

### Transaction Laundering

Front companies that appear to be legitimate businesses but exist to facilitate illegal transactions.

### Fake Accounts

Accounts created solely to process fraudulent transactions before closing down, leaving the merchant acquirer liable for chargeback costs.

### Synthetic Fraud

To evade sanctions and AML/TF laws, merchants use stolen identities to open accounts seeming to originate from another country or organization.

### Chargeback Exposure

Merchant acquirers are obligated to refund the issuing bank. If the merchant is unable to pay, they are left with the cost.

## How GeoGuard's fraud-checked advanced geolocation can protect merchant acquirers.

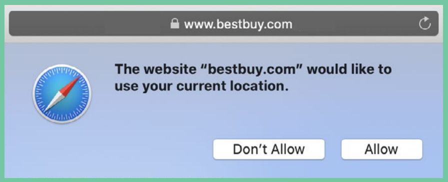
By integrating GeoGuard's geolocation anti-fraud solutions, merchant acquirers are able to embed advanced geolocation checks seamlessly into their user flows. This mitigates risk while maintaining a quick, automated sign up experience.

For instance, to combat synthetic fraud, the merchant acquirer requests that merchants verify their true location during the onboarding process. The merchant accepts the request and their location is verified as matching the country or business address. Future logins from new devices may also be verified geographically to ensure ongoing due-diligence.

By utilizing GeoGuard's solutions, potential fraudsters are required to provide their true geographic location, typically to within 100 meters, removing the online anonymity that protects them. This 'inconvenience factor' and location transparency is often enough for fraudsters to look elsewhere for easier targets.

### Location Access is the Norm

Asking to access device location data is very common on websites and causes minimal friction to the user experience.



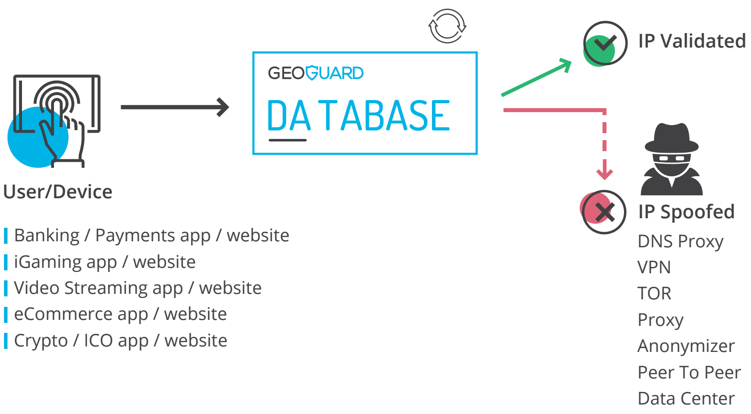
The website "bestbuy.com" would like to use your current location.

# DATABASE

*"Empowering the Future of Digital Trust"*

## Locally or API Hosted Fraud Protection

GeoGuard Database is our most simple to integrate solution and provides a seamless user experience. It comprises either a locally or API hosted fraud database of masked IP addresses. Unlike mainstream IP databases, GeoGuard provides multi-layered fraud protection against VPNs, proxies, peer-to-peer networks and other types of data manipulation. Our solution is continuously updated as new threats and data centers are identified and mitigation methods are developed.



- Banking / Payments app / website
- iGaming app / website
- Video Streaming app / website
- eCommerce app / website
- Crypto / ICO app / website

DNS Proxy
VPN
TOR
Proxy
Anonymizer
Peer To Peer
Data Center

GeoGuard's Database solution uses a single line of code for blocking VPNs, Proxies and Tor exit nodes. This service enables eCommerce platforms, merchant acquirers/PayFacs and other companies in the payments processing ecosystem to make better data driven decisions by screening users for signs of IP based geolocation fraud before applying regulatory, compliance or business rules.

### PRODUCT FEATURES

- Multi-layered fraud detection of VPNs, Proxies, etc.
- Fast & flexible integration options
- Multiple file formats supported

### LOCATION CONFIDENCE

- Minimize false positives
- Independently tested and validated by Cartesian and Kingsmead Security

### FRAUD STATISTICS

- 1 in 4 web users use a VPN on a daily basis
- Illicit actors use VPNs to hide their location while commiting fraud

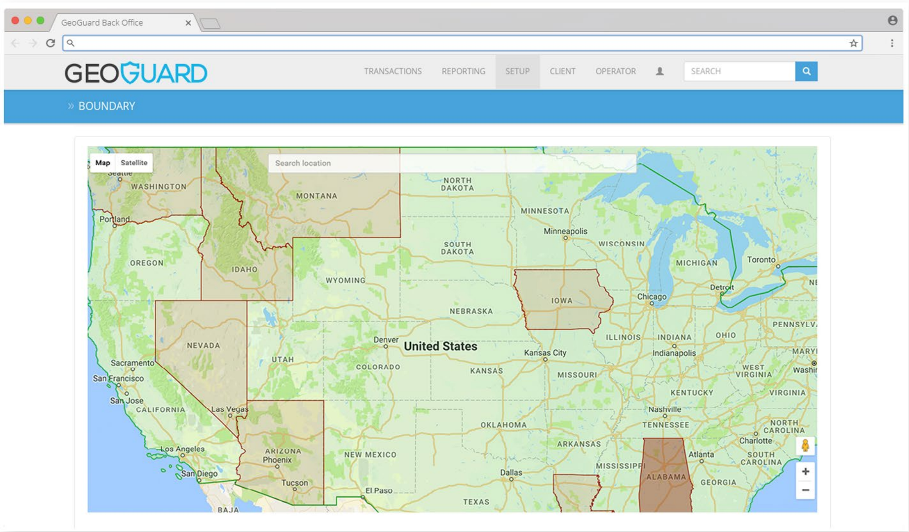
# SOLUS

*"Empowering the Future of Digital Trust"*

## No Download Browser Solution

GeoGuard's Solus offers a no-download geolocation solution that works directly within a company's website  and provides support for all devices and user interfaces.

For spoof-proof geolocation within the browser, this HTML5-based geolocation experience can be customized according to the security and licensing compliance needs of the particular company, with adaptable and configurable end-user prompts along with the secure collection of location data.



## Flexible Location Confidence

Solus is designed to counter the emerging location spoofing threats that previous generations of geo-fraud tools are no longer able to protect against – all from within a company's browser-based applications. By integrating GeoGuard Solus into a merchant acquirers' onboarding process, they are able to embed advanced geolocation checks seamlessly into their user flows.

## PRODUCT FEATURES

- Locate users on any device, app, or browser
- No download, low-barrier location method with flexible UX & custom alerts
- Embed into any webpage with a single Javascript file
- Highly scalable for a wide range of PayFac and payments processing environments

## LOCATION CONFIDENCE

- Used by companies around the world to protect against geolocation fraud
- Independently tested and validated by third-parties

## FRAUD STATISTICS

- Location spoofing technologies such as VPNs and Proxies are used worldwide by fraudsters to hide their true location
- Legislation is being introduced worldwide to include location data to strengthen  KYC and AML requirements

**Contact us to get started:** solutions@geoguard.com | geoguard.com

TrueLocationAPI

*"Empowering the Future of Digital Trust"*

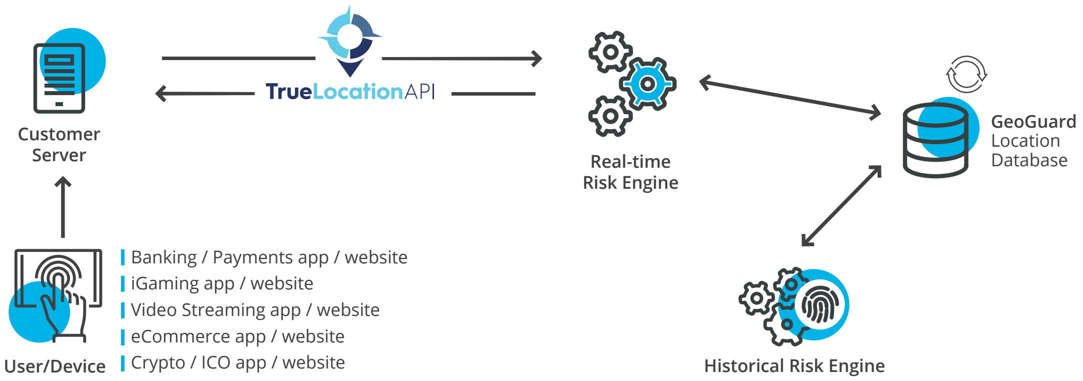
## Fraudulent Location Detection in Milliseconds via API

GeoGuard TrueLocation API provides advanced location-based fraud detection, utilizing both a real-time risk engine and a historical risk engine to identify and flag potential fraudulent activity. By analyzing both real-time and historical data, the GeoGuard TrueLocation API can help organizations easily identify and stop a wide variety of fraud including chargeback fraud, account sharing, CNP fraud and account takeovers.

GeoGuard TrueLocation API's rules are fully customizable, to meet an organization's unique requirements in terms of the amount of user data submitted, the types of flags generated and the fraudulent activities they are looking to identify and stop.

## PRODUCT FEATURES

- Detect and control account sharing via API
- Extremely easy to deploy as an API based solution
- No end-user friction, seamless experience via app or website
- Works with IP, HTML5 and native app geolocation data



## Real-Time Risk Engine Detects

- Faked lat/long coordinates from location apps running on the device
- The use of VPNs or DNS Proxies via the device's IP address
- Whether IP location and the location data submitted by the device are different
- Whether the lat/long is in a remote area where no people are living

## Historical Risk Engine Detects

- Account sharing when a user's lat/long coordinates jump a large distance in a short period of time
- Account sharing when a user's IP-based location coordinates jump a large distance in a short period of time
- Location spoofing if lat/long/accuracy are constant for a long period of time with multiple transactions
- Location spoofing when the data from multiple transactions has the same accuracy as used by location faking apps

**Contact us to get started:** solutions@geoguard.com | geoguard.com