# Fraud and Identity Theft Prevention By Using an IP Location Database

Posted on January 31, 2020

Offering high-quality customer experience (UX) often means personalizing and customizing products and services. Businesses have to collect personally identifiable information (PII) from customers, such as date of birth, credit card details, addresses, and other information. This is also the kind of data fraudsters are after so they can carry out identity theft.

Identity theft isn't even a new crime, which sprung up from the digitalization of business processes. It has been around since the early 1900s. Until recently, fraudsters emptied contents of garbage bins to find copies of legal documents with personal information.

These days, fraudsters don't even have to stand up and get out of their houses to obtain PII. Even script kiddies can launch cyberattacks to instigate fraud — thus making it every time more necessary to protect customers. Let's see why doing so matters in this post as well as look at how an IP geolocation data feed can help in the process.

## Why Do Companies Need to Protect Customer Data?

Businesses need to secure customer data for the following reasons:

- **Their brand reputation is on the line:** A data breach can negatively affect a company's brand reputation. It also alludes to providing poor customer service.

- **They are legally bound to protect PII:** In the U.S., almost every state implements laws that require businesses to immediately notify their customers when their PII is stolen or compromised. There are also different state and federal laws and industry regulations regarding the collection, use, and disclosure of PII. Businesses operating in or serving people in the European Union (EU) and European Economic Area (EEA), meanwhile, are bound to comply with the General Data Protection Regulation (GDPR) as failure to do so results in paying costly administrative penalties.

- **They could suffer significant financial losses:** A study by the Ponemon Institute revealed that publicly traded companies experience a 5% stock market price decline immediately after

suffering a data breach. Also, 27% of consumers whose data are lost in a breach stop doing business with the affected organization.

In short, there is definitely a need for organizations to take proactive steps in securing PII and other consumer data by strengthening their security infrastructure. Let's now talk about how IP location can be useful in that regard.

## IP Location Databases Help Prevent Unauthorized Access

An **IP location database** can fortify your digital infrastructure in three ways:

### Verify User Identity

With an **IP location database**, you can cross-check a user's current location against existing records to verify his identity. If the locations don't match, a user can be asked to complete other verification steps, such as answering security questions or entering a code sent to his email address or phone number. Although this process may burden customers who need to access their accounts from a different location, it ensures that unauthorized access doesn't happen.

### Block Anonymous Visitors

People are very concerned about their privacy and rightly so. Some of them want to browse the Web anonymously for fear of being tracked by cybercriminals, their ISPs, or even their own government. This trend resulted in around 26% of Internet users worldwide using VPN or proxy services to browse the Web.

The question then is this: why would companies want to block anonymous visitors when people only want to protect their privacy? Here are two major reasons:

- 50% of VPN users say that accessing restricted entertainment content is their top reason for using VPN. So, it's not even about avoiding government surveillance or hiding from cybercriminals. Companies that rely on IP geolocation to provide content for every region can also use an IP geolocation database to block VPN and proxy users.

- 69% of open proxies are bad proxies. Out of the 13,307 proxy services tested, 2,747 even modify sites' JavaScript while 2,391 change HTML content. These modifications are done to inject ads into the sites or, worse, steal cookies to get visitors' login information. Since it's quite daunting for companies to set different access rights for bad and good proxies, it's likely to be a wise business decision to block all users that use proxy services and do so with the help of an IP geolocation database.

### Filter Bad IP Addresses

Lastly, companies can block IP addresses with low reputation scores or that are associated with malware and other suspicious activities. IP Geolocation API has an exhaustive and accurate collection of IPv4 and IPv6 addresses amounting to 99.5% of all used IP addresses. This IP geolocation data can be compared with known indicators of compromise (IoCs) for the identifying and blocking of bad IP addresses.

To sum up, companies have the legal, moral, and ethical responsibility to protect the PII of their customers and employees. Failing to do so not only results in costly penalties but also in damage to reputation. An **IP location database** may help beef up an organization's threat intelligence and security platforms by preventing unauthorized access, and ultimately, fraud and identity theft.