MaxMind minFraud

Protection in Numbers

MaxMind minFraud Fact Sheet

MaxMind®

Working Together

Today, fraudsters can obtain all the information they need for identity theft, allowing them to bypass traditional verification tools. Even if they are caught at one site, they can simply move on to the next.

To address this issue, MaxMind has created a cross industry and non-intrusive fraud detection solution by combining IP geolocation, proxy detection and a mutual collaboration network. The network indirectly links thousands of merchants, allowing MaxMind to quickly uncover emerging fraud trends and suspicious behavior. Changes are made to the system to protect all merchants within the network in real-time. MaxMind currently screens over 110 million transactions per year with a risk model derived from over 200 million historic transactions.

Key Features

IP Geolocation provides the geographical location of the customer down to the city level and makes it easier to identify legitimate customers.

Proxy Detection determines the riskiness of IP addresses and whether or not they are anonymizing proxies.

BIN Number Check returns the country location of the creit card's issuing bank.

The minFraud Network is a reputation network that provides risk analysis based on historic legitimate and suspicious behavior for transaction attributes such as IP address, domain, and e-mail address.

Key Benefits

Non-intrusive: doesn't require customer to submit additional information

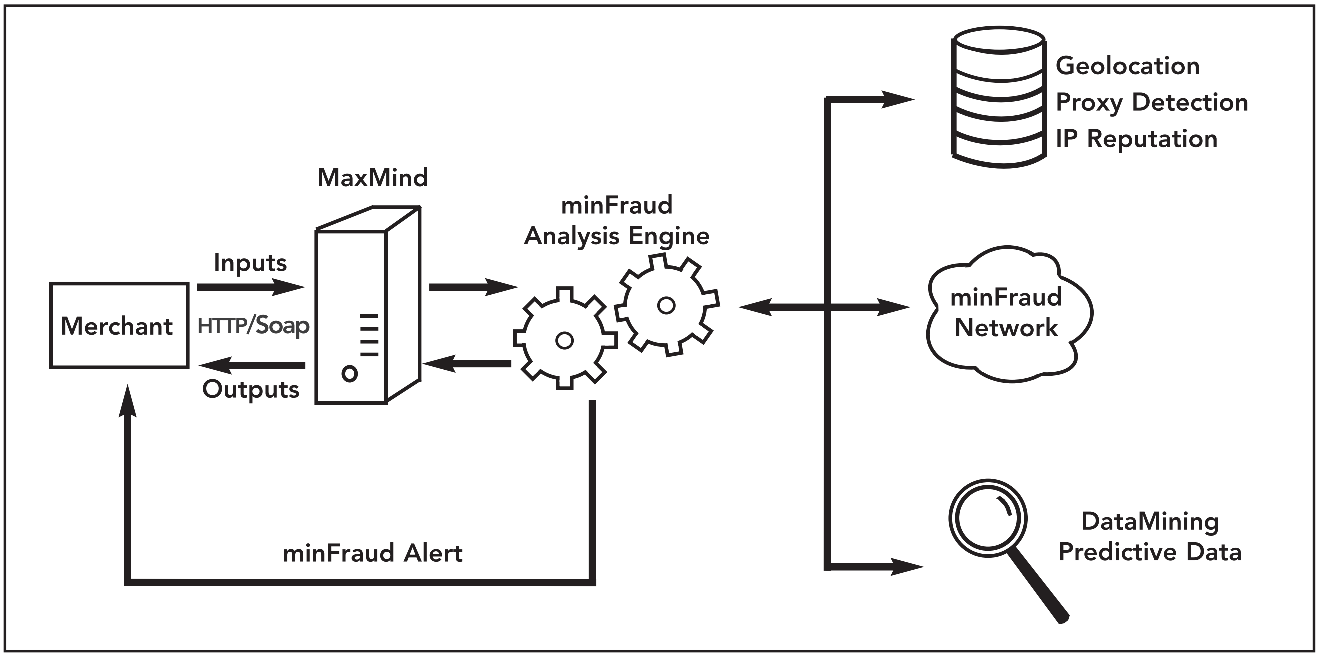
Privacy Protected: no personally identifiable information collected

Flexible: works with alternative payment options like PayPal, Google Checkout, and Bill Me Later

International: effectively screens transactions from any country

Modular: works with existing in-house or 3rd party solutions

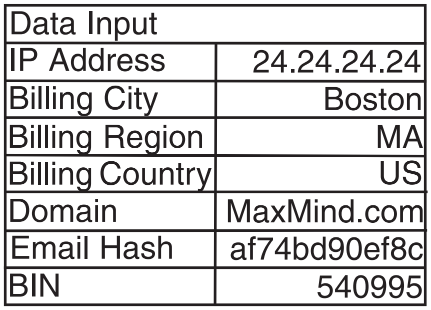
How it works



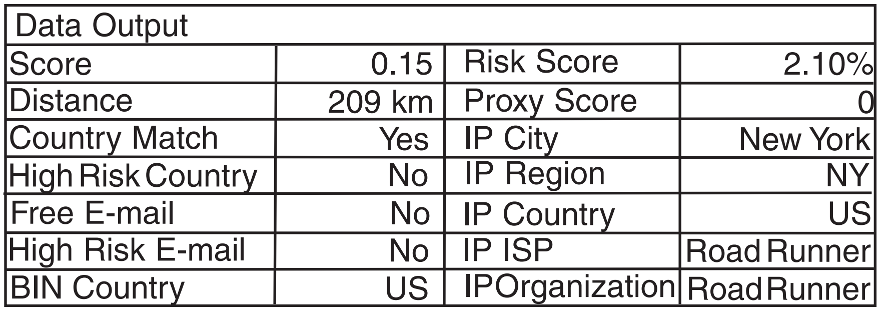
1. Merchant sends select transaction data to MaxMind using HTTP or SOAP.
2. MaxMind analyzes the transaction with different tools and sends data back to merchant.
3. Merchant then uses the data to decide how to process the order.
4. MaxMind continues to analyze the transactions for 2 weeks. Given new information and analysis, if fraudulent activity is uncovered, a "minFraud Alert" e-mail is sent out for the associated transactions.

What the data looks like:

The minFraud service returns two risk scores based on two separate models suitable for different types of businesses as well as various data pieces that can be used to create internal custom rules.   The following table shows a sample of the main data inputs and outputs.



Data Input	
IP Address	24.24.24.24
Billing City	Boston
Billing Region	MA
Billing Country	US
Domain	MaxMind.com
Email Hash	af74bd90ef8c
BIN	540995



Data Output			
Score	0.15	Risk Score	2.10%
Distance	209 km	Proxy Score	0
Country Match	Yes	IP City	New York
High Risk Country	No	IP Region	NY
Free E-mail	No	IP Country	US
High Risk E-mail	No	IP ISP	Road Runner
BIN Country	US	IPOrganization	Road Runner

Results

Many merchants that have implemented minFraud have seen a significant reduction in chargebacks and other costs associated with fraud. In some cases, the number of fraud attempts decreased over time as fraudsters migrated to other sites. Utilizing the risk scores and data elements of minFraud to automate the screening process, merchants typically see a reduction in the number of orders that need to be manually reviewed as well as the amount of time needed to review each order. The minFraud service provides merchants with an adaptive and ongoing strategy against fraud through the reputation and mutual collaboration network.

Signing up is simple and straightforward. Merchants can request a trial account to see how minFraud would address their own fraud issues. For more information, e-mail sales at sales@maxmind.com or call 617-500-4493 x805.