

WHITE PAPER

minFraud®

Prevent online fraud and reduce manual review using the minFraud service

MINFRAUD WHITE PAPER SUMMARY

The purpose of this white paper is to describe how the minFraud service can help your company protect itself from online fraud and help you determine if it is the right solution for you.

A Short History of MaxMind

In 2002, MaxMind began providing IP intelligence through the GeoIP® brand. Two years later, using GeoIP data, MaxMind developed the **minFraud**® service to combat the growing threat of online fraud. Since then, MaxMind has helped thousands of companies cut down on fraud-related financial losses and chargebacks, and has reduced these companies' need for manual review of transactions.

What does the minFraud service do?

MaxMind's minFraud service helps web-present businesses prevent online fraud by determining the riskiness of online transactions. It provides actionable data to identify and prevent online fraud for e-commerce transactions and account registrations. Each transaction sent to the minFraud service is assigned a riskScore, the probability that the transaction or registration is fraudulent. Companies use the riskScore to determine whether to accept, reject, or manually review transactions.

How the minFraud Service Works

minFraud service customers pass the service information provided by their site visitors during online transactions and account registrations. The minFraud service analyzes this information and returns a riskScore.

The minFraud service is a hosted solution that is accessed via an API. The only required inputs are the customer's IP address and non-street location information, but the service can take a number of optional inputs, which can result in more accurate scoring.

OPTIONAL INPUT EXAMPLES INCLUDE:

- EMAIL ADDRESS (HASHED)
- USERNAME AND PASSWORD (HASHED)
- DOMAIN OF EMAIL ADDRESS
- SHIPPING ADDRESS

- BANK IDENTIFICATION NUMBER (FIRST 6 DIGITS OF CREDIT CARD)
- AVS/CVV CHECK RESULTS
- USER-AGENT HTTP HEADER

For a full list of minFraud inputs, please visit - http://dev.maxmind.com/minfraud/

THIS IS A VISUALIZATION OF THE minFraud PROCESS FOR AN E-COMMERCE USE CASE. STEPS 2 TO 6 OCCUR IN LESS THAN A SECOND.



The riskScore

The riskScore – This is the most actionable piece of data companies receive from the minFraud service. It ranges from 0.01-100.00 and represents the probability that a given transaction is fraudulent. The riskScore takes into account a multitude of factors based on every transaction the minFraud network sees. On top of this, it also utilizes reputational information from the over half a billion historic transactions scored by the service in the past twelve months.

The risk model behind the riskScore is designed to recognize fraudulent behavior and adapt to emerging fraud patterns. Below, you will find the elements that go into the riskScore as well as some of the "questions" the minFraud service asks when coming up with a determination.

minFraud RISK MODEL ELEMENTS

GEOLOCATION CHECKS

Is there a significant mismatch between where an individual is and where they should be?

A fraudster with stolen credit card details is often forced to make transactions some distance away from the actual legitimate cardholder's country, region, or city of residence. IP geolocation checks detect this.

PROXY DETECTION

Are there legitimate reasons behind online visitors masking their IP addresses?

Proxies give web visitors the ability to mask their true IP address. The minFraud service can distinguish between legitimate proxies, such as those in office environments, and high-risk proxies frequented by fraudsters trying to obscure their true locations.

CREDIT CARD AND ISSUING BANK CHECKS

Is the issuing bank of a credit card in the country where the individual is?

Similar to the geolocation check, this feature can check whether an individual making a purchase is located in the same country as the bank that issued the credit card.

ONLINE REPUTATIONS

Has an IP address or email address historically been associated with fraudulent activity?

By tracking unique identifiers like IP address and email address over time, the minFraud service is able to detect fraud patterns and recognize if new transactions are associated with identifiers that been linked to fraud in the past.

DEVICE TRACKING

Is someone cycling through multiple proxies from a single device in an attempt to bypass IP geolocationbased anti-fraud measures?

Device tracking helps the minFraud service determine if fraudsters are quickly cycling through proxies in an attempt to bypass geolocation checks. This is accomplished by creating anonymous profiles of devices engaging in online web activity (e.g., making purchases).

Data for Decisions

Aside from the riskScore, the minFraud service also provides several outputs that can be used to build custom rules or help in manual review. Additional data returned by the minFraud service include all the GeoIP data MaxMind associates with the IP address provided, such as:

- Country, Region, City, ISP, Organization, Domain name, Netspeed, User-type
- Location data confidence factors, accuracy radius, and more

In addition, certain flags, which can be helpful in manual review or building custom rules, are returned if specific situations are encountered, such as:

- High-risk country: if the IP address is coming from a country which has historically been associated with risky/fraudulent activity.
- Anonymous proxy: if the IP address location is being masked by an anonymous proxy, which indicates a high risk of fraud.
- Corporate proxy: if the IP address location is being masked by a proxy, but is determined to be coming from a corporation/organization, which is a lower-risk indicator.
- Free e-mail address: if the domain of an email address passed through indicates that the email address is provided for free.

minFraud SERVICE KEY FEATURES

FRONT-LINE DEFENSE

The minFraud service works best as a front-line defense. The service's effectiveness and low price point mean most minFraud users put it first in their fraud-screening chain, using the minFraud service to significantly narrow the range of transactions passed to more expensive validation tools or sent for manual review.

STAND-ALONE OR COMPLEMENTARY

The minFraud service can work as the sole automated element in a fraud prevention system or in conjunction with other automated fraud solutions to better refine decisioning. The amount of integration work required to use the minFraud service is minimal, and it can easily be added or removed from a complex fraud process.

COMPLEX RULES, SIMPLER DECISIONS

Employing state-of-the-art statistical modeling and supervised machine learning, the minFraud service simplifies the decisions companies have to make. Insights that would otherwise be inaccessible are leveraged in order to provide the riskScore, an actionable data value that represents the risk of fraud.

SEAMLESS

The minFraud service works behind the scenes and is invisible to end-users. This means fewer hoops to jump through and less risk of web activity abandonment.

NETWORK EFFECT

Anonymous data-sharing affords mutual protection across the minFraud network, giving each customer access to decisioning that leverages the data of all minFraud service customers.

CHARGEBACK REPORTING

minFraud service users have the option of reporting instances of fraud via an API, which helps in tuning the algorithms behind the riskScore and reducing fraud even more in the future.

Getting Started

Is the minFraud service the right solution for me?

Today, the minFraud service screens more than 45 million online transactions per month for 7,000 companies using a risk model that is derived from over half a billion recent transactions. Through the riskScore, minFraud identifies about 5 million high-risk transactions per year across its user base.

Whether you are looking for a single solution or a front-line layer of protection against fraudulent online activity, the minFraud service can deliver the results and return on investment you are looking for. MaxMind is committed to delivering value and preventing online fraud in a manner that is cost-effective and simple. No start-up costs. No minimums. No forced ecosystem buy-in.

How to test the minFraud service

If you are interested in testing the service, you can sign up for a free trial at our website (<u>http://www.</u> <u>maxmind.com/minfraudtrial</u>). In addition, we're happy to do historical testing of past transactions to see how the service would have scored transactions you know to be legitimate or fraudulent. Please contact one of our sales representatives to see if historical testing is right for you.

HOW TO GET STARTED

127.0.0.1

If you'd like to get started, you can integrate the service yourself or "turn it on" within certain carts or e-commerce platforms.

http://www.maxmind.com/en/ccv_buynow	To make a purchase of queries to begin using the minFraud service today.
dev.maxmind.com	For more technical details and integration assistance.
sales@maxmind.com	To get in touch with a sales representative.

Partner with us

E-commerce platforms, payment processors, payment gateways, and other platform solutions providers, we'd be happy to help deliver the value of the minFraud service to your clients.

Please email partner@maxmind.com to discuss partnership opportunities.



24 CRESCENT STREET, SUITE 301 WALTHAM, MA 02453 1 (617) 500-4493 WWW.MAXMIND.COM