

Fraud Detection through IP Address Reputation and a Mutual Collaboration Network



MaxMind White Paper



■ About this White Paper

MaxMind developed minFraud®, a non-intrusive online fraud detection solution based on the combination of IP reputation analysis and a mutual collaboration network. IP reputation takes geolocation and proxy detection to the next level by providing relevant information about the IPs' historic behavior, legitimate and suspicious. The minFraud service allows online merchants to indirectly share non-personally identifiable but relevant fraud information with other merchants for mutual protection through the minFraud Network. Today, MaxMind screens over 200 million online transactions a year for a network of more than 10,000 merchants around the world. This white paper describes how various components of MaxMind's IP reputation technology and mutual collaboration network provide a more adaptive, dynamic, and ongoing strategy for fraud detection.

■ IP Reputation: The Foundation of minFraud

Given the Internet's built-in anonymity and the ability to execute transactions from anywhere, authenticating the identity of the customer can be fairly difficult. Traditional tools such as Address Verification Systems (AVS) and Card Verification Values (CVV) have become less effective since sophisticated fraudsters generally have access to complete credit card information of the individuals they are trying to impersonate. Other authenticating solutions may require customers to take additional steps, disturbing the seamlessness of the purchasing experience. Often, this leads to shopping cart abandonment.

Geolocation is the ability to determine where online visitors are physically located based on their IP addresses. With geolocation, merchants can use information they already have, the users' IPs, to non-intrusively determine where their customers are physically located. By creating geographic boundaries on the Internet and providing the customer's location, geolocation can be used effectively to detect potential fraud by analyzing the differences between the user location and the billing address. Building on geolocation, IP reputation provides relevant risk indicators on given IP addresses to supplement geolocation analysis (e.g., comparing IP location and billing address).

> GeolIP®: Taking Geolocation to the Next Level

MaxMind's geolocation technology, GeolIP, is tailored specifically for fraud detection applications due to the methods used to generate the data sets. MaxMind collaborates with websites where users are asked to "self-geolocate" themselves by providing their physical location, which we refer to collectively as user entered data. Examples of this are registrations for software products and online account creations.

The user's IP address and user entered data are forwarded to MaxMind after all personally identifiable information has been removed to protect the user's privacy. MaxMind then runs millions of these IP location pairs through a series of algorithms that scrub and extrapolate relevant location data. Less tractable IP addresses are manually reviewed resulting in resolutions with 99.8% accuracy on the country level and 93% on the US state level. On top of determining where IP users are coming from, over time, this methodology allows MaxMind to develop a reputation of each IP's usage given its historic activity.

> Anonymizing Proxies: Where Fraudsters Try to Hide

Pure geolocation controls have their limitations. Fraudsters can use anonymizing proxies to mask their true location as a way of bypassing geolocation controls, thus allowing them to pretend to be coming from anywhere in the world. In fact, fraudsters often are able to find proxies that are located within the same state or city as the billing address. The ease with which fraudsters can switch between proxies and assume the IP address of a hijacked computer makes proxy detection an integral part of any fraud detection system. Incorporating proxy detection provides an additional layer of protection when used in conjunction with geolocation controls or other solutions.

MaxMind spends considerable resources and uses a variety of methods to identify and track anonymizing proxies. By building on top of GeolIP, MaxMind uncovers anonymizing proxies by

analyzing the deviations and irregularities between transaction data (e.g., billing address), an IP's expected behavior, and other relevant IP information (e.g., ISP, netblock owner, etc). In addition, MaxMind incorporates several third party data sources that provide additional risk indicators to complement internal analytics used during automated and manual review. Approximately 32% of the highly suspicious transactions flagged by MaxMind come from anonymizing proxies.

minFraud Network: Protection in Numbers

Rather than building higher walls for individual sites, MaxMind focuses on the the development of the minFraud Network, a distributed protection system that allows thousands of participating members to indirectly share non-personally identifiable but relevant fraud information for mutual protection. The minFraud Network complements the data that is being provided through IP reputation. If suspicious behavior is uncovered at one merchant site, changes are made to the minFraud system to protect other merchants within the minFraud Network in real-time. Additional feedback from merchants helps serve as warning signals to others within the network. Since chargebacks can happen for a variety of the reasons, often not related to fraud, MaxMind reviews all feedback provided by merchants to ensure that only appropriate fraud data is incorporated into the network.

Pro-Active Analysis: Uncovering Emerging Fraud Trends and Risks

MaxMind analyzes and data-mines transactions from the entire network through a series of automated and manual review processes. The review processes incorporate IP reputation and proxy detection analysis, but on a network level rather than at the individual merchant level. Where one merchant may see one transaction over one IP address, MaxMind may see twenty transactions over the same IP from twelve merchants, making it easier to detect suspicious behavior or emerging threats.

MaxMind also investigates associated transactions of flagged orders to uncover additional suspicious activity. For example, if a domain was flagged as having a bad reputation, MaxMind will review all the IP addresses or other attributes associated with orders placed from the flagged domain. This allows MaxMind to uncover additional suspicious activity and derive additional predictive risk factors for future transactions. Often, one or two fraudulent transactions can lead to hundreds of related transactions through association as fraudsters try to make repeated purchase attempts with similar order characteristics.

> Reputation Platform: Tracking Historic Legitimate and Suspicious Activity

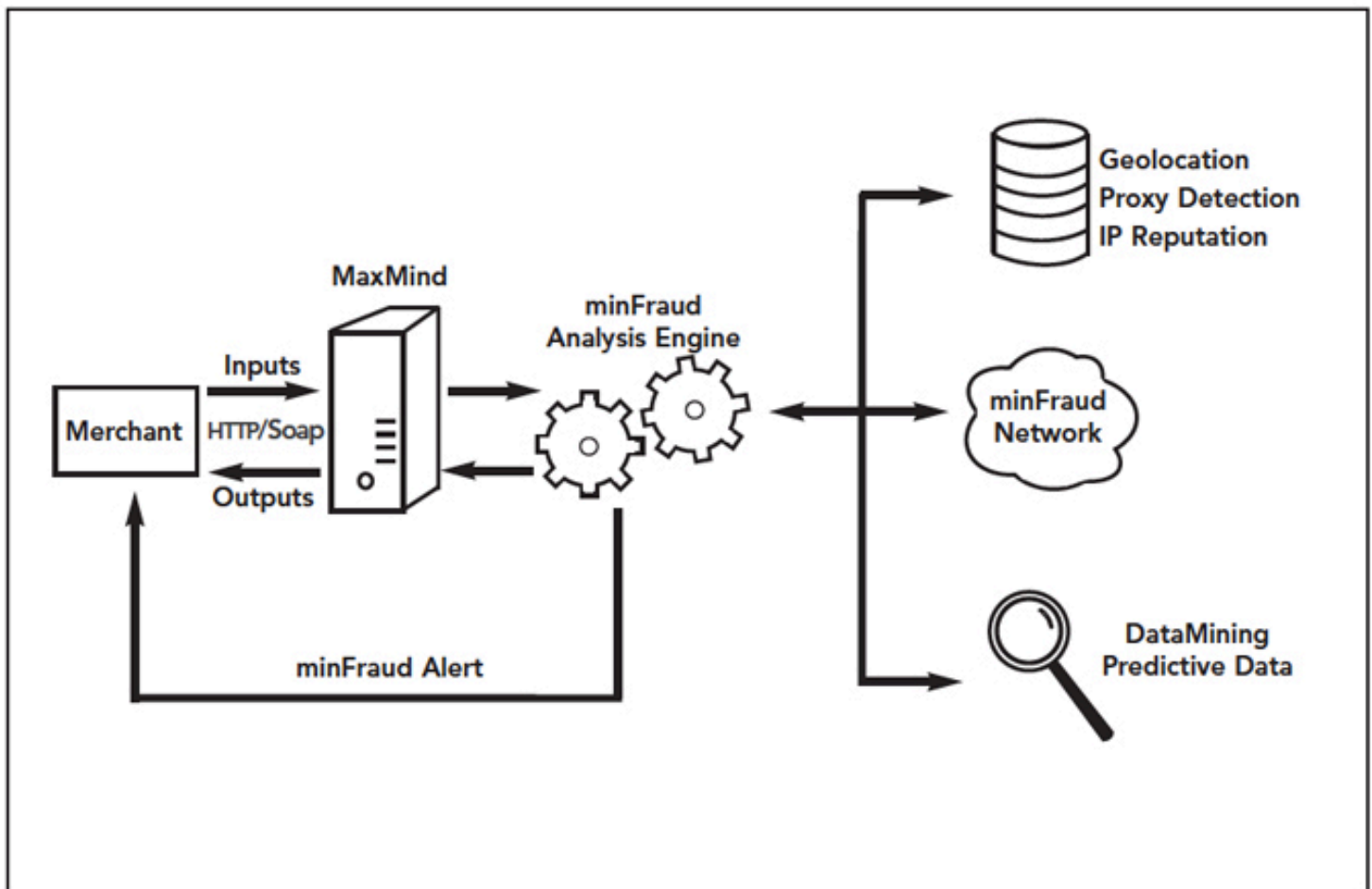
The minFraud Network is a platform for developing reputation indicators for characteristics associated with online purchases. Reputation can be positive or negative depending on inherent and observed historic activity. MaxMind has developed reputations for IP addresses, anonymizing proxies, corporate proxies, online domains, organizations, hashed e-mails¹, satellite providers, and hosting providers through the analysis of hundreds of millions of historic online transactions. The reputation data derived from the analysis is incorporated into the risk assessment of current transactions and presented in aggregated form through certain service output fields.

MaxMind continues to monitor transactions for up to two weeks. As more information comes into the minFraud network, MaxMind may change its initial risk analysis. If transactions were deemed to be highly risky after the initial query, an alert is sent to the merchants notifying them of the analysis and reputation change. This allows merchants to mitigate losses by stopping the shipment of physical goods or closing down affected accounts for digital merchants. On average, alerts are sent out within six hours of the initial query allowing for a quick response on the merchant end.

¹ Merchants can pass MaxMind the MD5 hash of the customer's e-mail address. This allows MaxMind to have a unique identifier to track the reputation of the e-mail without actually knowing what the e-mail address is.

How minFraud Works

The minFraud Service is a web service that can be queried via the HTTP protocol (APIs available in PHP, Perl, and Java languages) or by using SOAP. Merchants are not required to ask customers for any additional information since the data service inputs are the same as those of typical online order forms. Within one second, MaxMind returns a risk score as well as other relevant raw details on the analysis of the transaction. The outputted data can be used to automate order processing or used to supplement manual review.



Conclusion

MaxMind offers merchants the ability to implement a fraud detection solution from a different angle, through IP reputation. The combination of IP reputation and the minFraud Network provides merchants with an ongoing and long term strategy against fraud. The minFraud service can be used as a stand-alone solution or as a modular component to complement existing fraud systems in the B2B and B2C space. It has been used successfully by thousands of merchants to screen transactions from credit cards, PayPal, Google Checkout, and other online payment methods. Merchants that have implemented minFraud have seen a large reduction in costs associated with fraud and chargebacks. In addition, minFraud reduces overhead costs associated with manual review by cutting the number of transactions that need to be reviewed as well as the time it takes to review each transaction.