

Blackbaud Merchant Services™ Fraud Management Risk Score Factors

How Blackbaud Merchant Services Determines the Risk for Fraud

For organizations that require additional fraud prevention for credit card processing, **Blackbaud Merchant Services** offers a premium **Fraud Management** service. Through the web portal, you can enable and configure **Fraud Management** to provide comprehensive screening of Card Not Present transactions to help detect payment card fraud for a nominal per-transaction charge. With **Fraud Management**, **Blackbaud Merchant Services** evaluates many factors to determine the likelihood of transactions being fraudulent and assigns a risk score, from 1-100, to rate the risk of fraud. The higher the risk score, the greater the likelihood the transaction is fraudulent. For example, a transactions with a risk score of 30 has a 30% chance of being fraudulent.

In the **Blackbaud Merchant Services** web portal, the default risk score threshold is 35, based on the historical analysis across thousands of transactions. If a transaction's risk score is greater than 35, **Blackbaud Merchant Services** automatically declines it as fraudulent. We recommend you adjust the threshold as necessary to best meet your needs. For example, to tighten the fraud screening, you can lower the risk score setting from the **Fraud Management** area of the portal.

There is no static formula to calculate the risk score. To determine the risk score, **Blackbaud Merchant Services** considers several risk factors and statistical fraud patterns such as bank identification number (BIN) country match, proxy detection, billing information checks, and IP address information.

Bank Identification Number Country Match

Cardholders rarely have a billing address in a country different than their credit cards' issuing banks. To verify the countries of the billing address and the issuing bank match, **Blackbaud Merchant Services** uses the first six digits of the credit card number, which are known as the Bank Identification Number (BIN) or Issuer Identification Number (IIN) and identify the institution that issued the card and its country of origin.

► A positive BIN country match does not necessarily indicate a valid transaction. Fraudsters may have access to limited and incomplete BIN lists and select to use corresponding credit card numbers.

To determine the risk score threshold that best meets your needs, we recommend you compare the average scores of your processed valid transactions and known fraudulent transactions to determine the maximum score and then routinely monitor and adjust accordingly based on the dynamic nature of fraud.

From the web portal, you can select to reject all transactions from billing address countries that do not match the issuing banks'.

Continued on following page

Proxy Detection

To determine the risk score, **Blackbaud Merchant Services** checks for anonymous or open proxies associated with the IP address.

- **Anonymous proxies.** Anonymous proxies are legal services that disable and prevent IP geolocation tools to provide anonymity to those concerned about online privacy. Fraudsters may use anonymous proxies to hide their true locations and bypass geolocation filters. Transactions received from IP addresses marked as anonymous proxies are considered to be high risk.
- **Open proxies.** Open proxies are computers or servers that have been hacked or infected with trojans or viruses such that users can connect to them without the owners' knowledge. Fraudsters may use open proxies to simulate transactions from the highjacked computers to bypass IP geolocation tools. **Blackbaud Merchant Services** evaluates the riskiness of an IP address, based on increased and inconsistent activities or an association with suspicious activities or chargebacks typical of an open proxy, to determine a proxy score that directly influences the overall risk score.

To help avoid fraudulent transactions, you can select to reject all transactions from anonymous proxies through the web portal.

Address, Email, and Phone Number Checks

For Card Not Present transactions from **Blackbaud NetCommunity** associated with known street addresses, phone numbers, and email addresses, **Blackbaud Merchant Services** evaluates this contact information to determine the risk score.

- **Phone number and ZIP Code match.** For phone numbers in the United States, **Blackbaud Merchant Services** determines whether the phone number is located in the ZIP Code of the billing address. However, a valid transaction may result in a mismatch, such as when the cardholder uses a cell phone with a prefix or local number exchange that does not match the ZIP Code. Similarly, a match does not necessarily mean a transaction is valid, as fraudsters may use Voice over IP (VoIP) numbers so the prefix and local number exchange match the ZIP Code of the billing address.
- **City/State and ZIP Code match.** Since the Address Verification Service (AVS) only checks to see if the ZIP Code matches the numeric portion of the street address, fraudsters may enter bogus values for the city and state when they test credit card numbers and check available credit limits. For addresses in the United States, **Blackbaud Merchant Services** determines whether the city and state of the billing address match the ZIP Code.
- **Free email domains.** **Blackbaud Merchant Services** determines whether the domain used for the email address is from a free email provider such as yahoo.com or gmail.com. While many donors likely use free email addresses, transactions from these domains are inherently more risky. Fraudsters typically prefer free email accounts, which are easily created or recycled and cannot be traced to their rightful owners. Statistically, free email addresses double the likelihood of fraud.
- **Carder email.** Since fraudsters often use the same email address multiple times, **Blackbaud Merchant Services** evaluates the address for previous fraudulent transactions or chargebacks.

Continued on following page

IP Address Information

To determine the risk score, **Blackbaud Merchant Services** evaluates the latitude, longitude, and several other factors of the IP address where the transaction originates.

- **Billing address country match.** For most transactions, the country of the IP address should match the country of the cardholder's billing address. However, a valid transaction may result in a country mismatch, such as when the cardholder is traveling or an organization has branches in multiple countries. Similarly, a country match does not necessarily mean a transaction is valid, as fraudsters may use anonymous proxies or services to create a country match.
- **Country code.** When the countries of the billing and IP addresses do not match, **Blackbaud Merchant Services** assesses risk based on where the transaction originates. For example, a transaction from the United Kingdom is typically less risky than one from Nigeria. In addition, the distance between the billing address and the country of the IP address may influence the risk. For example, a transaction with a billing address in close proximity to the IP address is less risky.
- **Distance.** Typically, a greater distance between the IP address and billing address indicates a greater risk of fraud. However, shorter distances do not necessarily indicate a valid transaction, as fraudsters may use proxies in close proximity to the billing address.
- **High-risk countries.** Some countries and regions have a higher risk for fraud in regards to scams and stolen credit cards. Due to a statistically high rate of fraudulent transactions from Ghana, Nigeria, or Vietnam, transactions with a billing or IP address in these countries result in higher risk scores.
- **Billing address region and city match.** If the region and city of the billing address matches the region and city of the IP address, the likelihood of risk is lower, if there is no indication of a proxy. If the region or city mismatch, **Blackbaud Merchant Services** evaluates the distance between the billing and IP addresses.

To help avoid chargeback requests and suspect transactions, you can select to reject all transactions from high-risk countries through the web portal.