Blackbaud Merchant Services™

Fraud Management and Prevention

Globally, credit card fraud is on the rise and the threat is greatest for organizations processing online (card-not-present) transactions. Blackbaud Merchant Services—Blackbaud's PCI-compliant payment processing solution—mitigates your risk by encrypting credit card data, automatically blocking transactions based on Internet-Protocol (IP) addresses or blacklisted cards, and providing additional fraud management tools.

Fraud Management Basics

Basic fraud management settings are configured within the Blackbaud Merchant Services Web Portal and include:

- **Card Security Code Check (CSC)**
  The CSC or Card Verification Value (CVV or CVV2) is a three- or four-digit number that appears on the credit card and nowhere else. It helps ensure that the person who makes the purchase or online donation has the physical credit card in his or her possession.

- **Address Verification Service (AVS)**
  AVS verifies the credit card billing address provided by the user matches the address on file with the credit card company.

- **Three-Domain Secure (3DS) Authorization**
  Used by major credit card brands, including Visa® and MasterCard®, this authentication standard requires cardholders to register their cards through the card issuer's website and specify credentials to be used for online transactions.

- **Suspect Transaction Notification**
  You can opt in to receive email notifications when a suspect transaction is flagged, such as a submission from a questionable IP address or multiple transactions from the same credit card within a short period of time.

Mitigate Fraud

Blackbaud Merchant Services protects your organization and your constituents from payment card fraud.

Learn more

Protection and Support Built for You

Blackbaud's Risk Management and Chargebacks team continually monitors Blackbaud Merchant Services accounts for fraudulent activity and works closely with clients and organizations—including the Internet Crime Complaint Center (IC3), a joint venture of the Federal Bureau of Investigation (FBI) and National White Collar Crime Center (NW3C)—to manage and report fraud.

Premium Fraud Management

If your organization has experienced fraud or a large number of suspect transactions, you can take advantage of premium Fraud Management. Designed for online transactions, this service is available to all users of Blackbaud Merchant Services. It can be started and stopped as needed, and our support specialists can recommend the optimal timing.

With premium Fraud Management, Blackbaud Merchant Services generates a fraud score based on the likelihood of the credit card transactions being fraudulent. Those transactions with the greatest risk are assigned the highest scores. You can then designate a maximum risk score for your nonprofit and automatically reject transactions that exceed the threshold. In addition, you can provide further customization by adjusting the settings for:

END-TO-END SECURITY AND ACTIVITY MONITORING

Blackbaud continuously works alongside your organization to recommend fraud-mitigation best practices that meet your organization's unique needs.

- **Anonymous Proxies**
  Anonymous proxies are used to help cybercriminals hide their true locations. Blackbaud Merchant Services lets you reject all transactions from anonymous proxies. It also tracks information about the devices used to submit online transactions and can identify when a scammer changes proxies while on a website or between visits to a donation page.

- **High-Risk Countries**
  Certain countries have a high risk of scams and credit card fraud. With premium Fraud Management, you can reject all transactions that originate in these countries.

- **Bank Identification Number (BIN) / Issuer Identification Number (IIN) Country Match**
  Blackbaud recommends that you reject transactions where the countries of the BIN or IIN—the first six digits of the credit card number—do not match the cardholder's billing address, since many international credit cards do not support AVS.

- **Account Velocity**
  Blackbaud Merchant Services can be set up to deny transactions based on the number of times the same card data—credit card number, card type, and expiration date—has been used within a short duration.