DATA SHEET

Preventing Fraud with Blackbaud Merchant Services™

Last year, costs for global payment card fraud reached nearly $17 billion. And trends show that number will exceed $35 billion in 2020. With more nonprofits falling victim to fraudulent credit card transactions, what can your organization do to protect itself?

Start by using Blackbaud Merchant Services, Blackbaud's end-to-end payment processing solution that's compliant with the Payment Card Industry Data Security Standard (PCI DSS). Blackbaud Merchant Services leverages the Blackbaud Vault to encrypt your donors' credit card data and remove your organization's risk of storing this information. Blackbaud Vault also protects you by automatically blocking transactions based on Internet protocol (IP) address and blacklisted credit cards.

Fraud Management Basics

Within Blackbaud Merchant Services, there are settings that can be configured to further reduce your risk, including:

- **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. In the Blackbaud Merchant Services Web Portal, you can select whether to use CSC checks and at what level.
- **Address Verification Service (AVS)**
  AVS verifies the credit card billing address. When you configure your Blackbaud Merchant Services account, you can decide to use AVS and set the level. Depending on your selection, Blackbaud Merchant Services will determine whether to accept the payment.
- **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. Blackbaud Merchant Services lets you choose 3DS as a fraud-mitigation option.

Protect your nonprofit from credit card fraud.

With Blackbaud Merchant Services, you can reduce your risk. Take advantage of the system's standard fraud-mitigation features, or subscribe to our premium Fraud Management service.

Learn More ➤

Our Payment Services support specialists will work alongside your nonprofit to recommend fraud-mitigation best practices that meet your organization's unique needs.

- **Suspect Transactions**
  From the Blackbaud Merchant Services™ Web Portal, you can opt in to receive email notifications when a suspect transaction is flagged. The system automatically flags these transactions when they meet a certain criteria, such as submission from a questionable IP address or multiple transactions from the same credit card within a short period of time.

Since Blackbaud Merchant Services is integrated with other Blackbaud solutions, you can also take advantage of the fraud-prevention features available in those systems. For example, Blackbaud NetCommunity™ supports CAPTCHA functionality to prevent fraudulent activity from automated programs called "bots."

Advice from the Experts

As a Blackbaud Merchant Services client, our Payment Services support specialists will recommend fraud-mitigation best practices. Along with our Risk Management and Chargebacks team, they continually monitor Blackbaud Merchant Services accounts for fraudulent activity and work 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 card-not-present (online) transactions, this add-on service is available to all users of Blackbaud Merchant Services for a nominal per-transaction fee. 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:

- **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.
- **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.
- **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.
- **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.

For more information on managing credit card fraud, email bbms@blackbaud.com. ➤