Blackbaud Merchant Services Web Portal Guide

09/24/2018 Blackbaud Merchant Services 4.0 Blackbaud Merchant Services Web Portal Guide US

Portal-2017

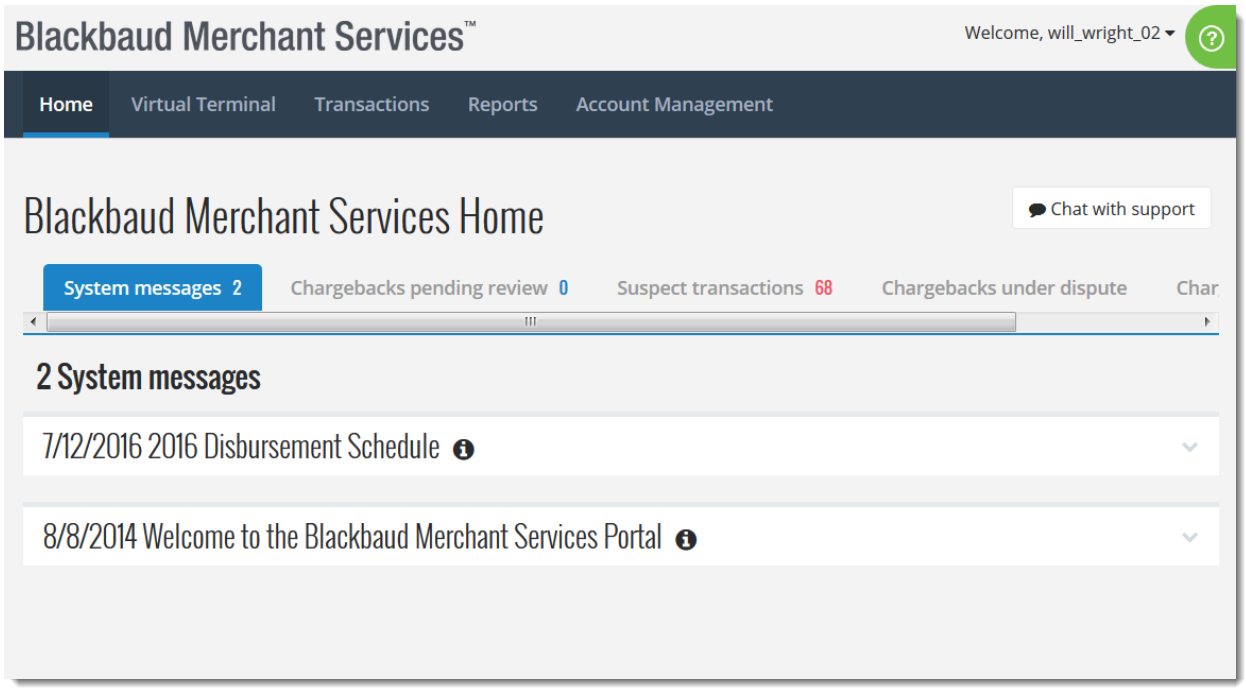
Contents

Home Page

When you log into the web portal, you first see the home page. Here, you can review system messages and navigate through the entire web portal.

The tabs on the home page include access to commonly used areas and tasks. Use the following tabs to see messages, manage chargeback transactions, and approve or reject transactions flagged as suspect by ***Blackbaud Merchant Services***.

To access the web portal, log into https://bbms.blackbaud.com. For optimal performance, we recommend you access the web portal through *Microsoft Internet Explorer* 8 or higher, or the latest versions of *Apple Safari*, *Mozilla Firefox*, or *Google Chrome*.



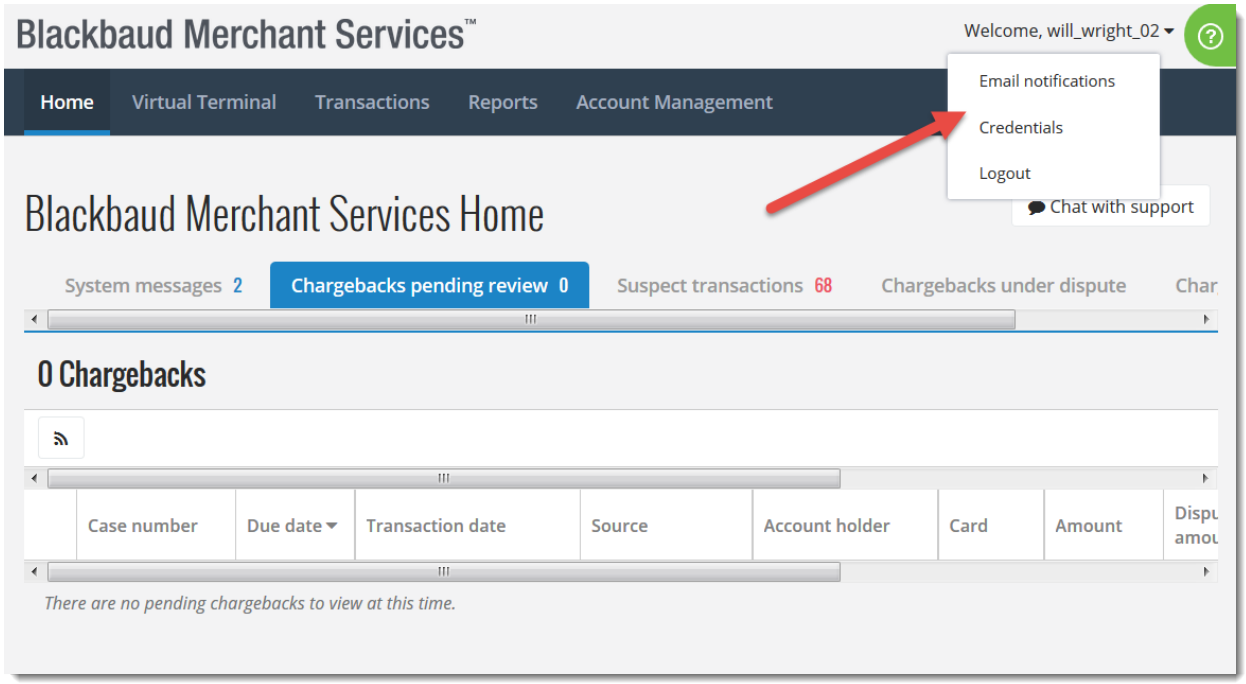
- **System messages:** You can expand system messages to review details. System messages are published by Blackbaud and provide you with important information about using the web portal and any relevant announcements.
- **Chargebacks pending review:** This tab includes any chargebacks that require your review. For more information, see Chargebacks Pending Review on page 27.
- **Suspect transactions:** This tab lists all transactions that are deemed suspect and require your review. This list includes transactions from the past 30 days. For more information, see Suspect Transactions on page 19.
- **Chargebacks under dispute:** This tab lists chargebacks that are currently under dispute and have

not yet been resolved. For more information, see Chargebacks Under Dispute on page 29.

- **Chargebacks resolved:** This tab includes all chargebacks that have been resolved. For more information, see Resolved Chargebacks and Direct Debit Returns on page 29.

User Settings

You can manage your user account from within the web portal. Under your user name at the top right of the screen, you can view and edit your credentials for ***Blackbaud Merchant Services*** and manage your email notifications about activity in the web portal. You can also set up email notifications for other users in your organization.



Blackbaud Merchant Services Credentials

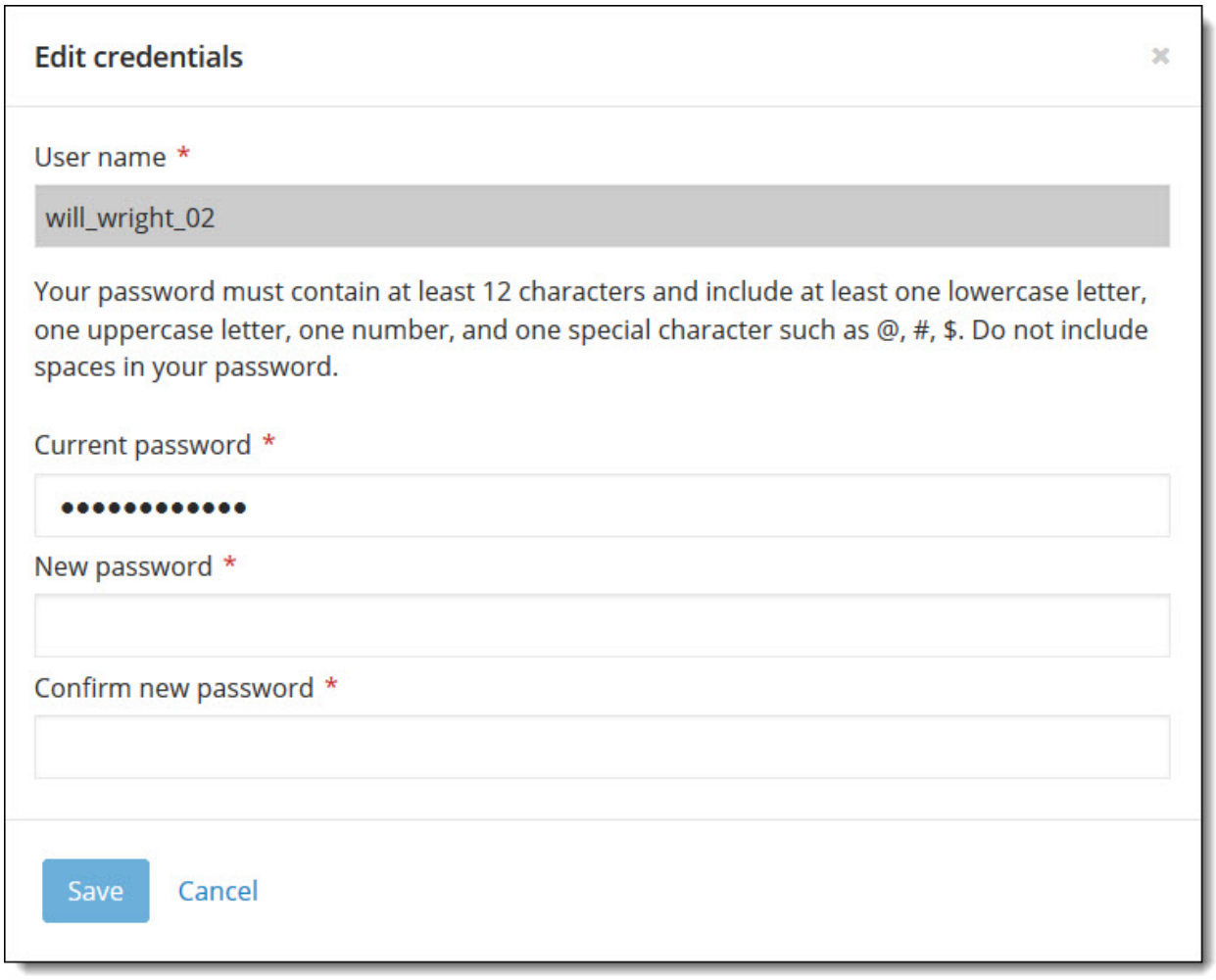
From the web portal, you can view and manage your login credentials to access your ***Blackbaud Merchant Services*** account. The Administrator credentials are used to connect to your merchant account in Blackbaud programs. To view and manage your credentials through the web portal, under your user name on the top right of the screen, click **Credentials**.

You can edit your password as necessary, such as for security reasons. After you edit your password, you must log back into the web portal.

Warning: If you change your ***Blackbaud Payment Service*** or ***Blackbaud Merchant Services*** passwords, you must also update all of your Blackbaud applications that use ***Blackbaud Payment Service*** or ***Blackbaud Merchant Services*** with the new credentials. If you do not, credit card and ACH (direct debit) transactions will fail to process.

Edit the Blackbaud Merchant Services password

1. Under your user name on the top right of the screen, click **Credentials**. The Blackbaud Merchant Services Credentials page appears.



2. Under **Current password**, enter the current password for your account.
3. In the **New password** and **Confirm new password** fields, enter the new password to use with your account.
4. Click **Save**. You return to the login screen for the web portal. To log in, enter your new credentials for ***Blackbaud Merchant Services***.

Email Notifications

From the web portal, you can select to receive email messages to inform you of activity within your ***Blackbaud Merchant Services*** account, such as specific types of transactions, disbursements, or account configuration changes. To select when to receive email messages, under your user name on the top right of the screen, click **Email notifications**. The Email Notifications page appears. For each

type of activity, click the ellipsis and click **Edit**. Then, specify the recipient email addresses and when they should receive notifications and click **Save**.

- For **Suspect transactions**, select whether to receive a summary of transactions that ***Blackbaud Merchant Services*** marked as suspect, such as due to questionable IP addresses or multiple identical transactions from the same credit card within a short amount of time. You can select to receive the summary on a daily or weekly basis. For information about how to manage suspect transactions, see Suspect Transactions on page 19.
- For **Online transactions**, select whether to receive a summary of processed card-not-present transactions, such as through a donation form on your website. You can select to receive the summary on a weekly or monthly basis.
- For **Mobile transactions**, select whether to receive a summary of processed ***Blackbaud MobilePay*** transactions. You can select to receive the summary on a daily, weekly, or monthly basis.
- For **Chargebacks**, select whether to receive notifications of chargeback requests received from the credit card company, such as when the card holder disputes the validity of the transaction. You can select to receive notifications as chargebacks occur, or you can receive a summary on a daily, weekly, or monthly basis. For information about how to manage chargeback requests, see Chargebacks and Direct Debit Returns on page 25.

Tip: To receive notifications when open or disputed chargeback requests are closed, select "As it happens" for **Chargebacks**.

- If your organization enables fraud management, for **Fraudulent transactions**, select whether to receive notifications when your account rejects transactions as fraudulent. You can select to receive notifications as fraudulent transactions occur, or you can receive a summary on a daily, weekly, or monthly basis. For information about fraud management, see Fraud Management on page 36.
- For **Disbursement reports**, select whether to receive notifications when new disbursement reports become available in the portal.
- For **Account management**, select whether to receive notifications of changes to the account's settings such as disbursement information, contact details, or users and roles. For information about these settings, see Account Management on page 33.
- For **Direct debit declines**, select whether to receive notifications of declined direct debit transactions, such as due to insufficient funds, a closed account, or incorrect account information. You can select to receive notifications as declined transactions occur, or you can receive a summary on a daily, weekly, or monthly basis.
- For **Direct debit returns**, select whether to receive notifications of direct debit transactions approved but then returned by the bank, such as when the account holder disputes the transaction. You can select to receive notifications as returned transactions occur, or you can receive a summary on a daily, weekly, or monthly basis.
- For **Large suspect transactions**, select whether to receive notifications when ***Blackbaud Merchant Services*** marks credit card or direct debit transactions as suspect due to unusually large amounts. For information about how to manage suspect transactions, see Suspect Transactions on page 19.
- If your organization subscribes to the Credit Card Updater service through a Blackbaud

application, for **Credit card updater**, select whether to receive notifications when your account receives updated card number or expiration date information in your Blackbaud programs.

Virtual Terminal

You can submit card-present transactions and card-not-present transactions through the web portal.

Note: To submit transactions directly through your account, you must first configure your ***Blackbaud Merchant Services*** account. For information about how to configure an account, see Account Configurations on page 38.

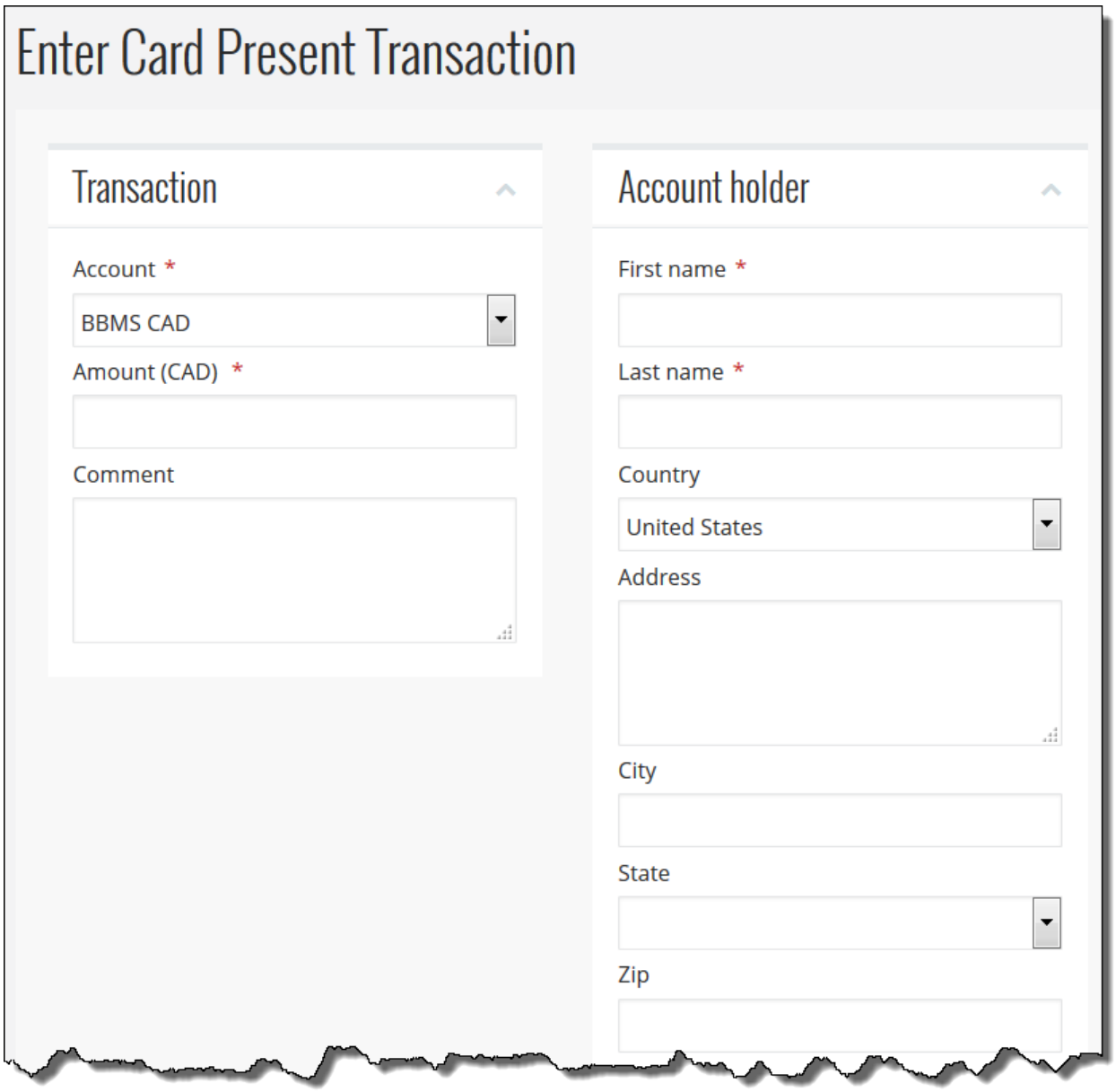
Card-Present Transactions

When you access the web portal through a workstation connected to a card swipe reader, you can submit card-present transactions to ***Blackbaud Merchant Services*** directly through the web portal. You can also select to manually enter the credit card information for the card-present transaction.

Warning: When you process a transaction directly through the web portal, no corresponding record of the transaction appears in the database of your Blackbaud program. To maintain a record of the transaction, such as to include in reports on giving or revenue activity, we recommend you enter and process transactions through your Blackbaud program.

Submit a card-present transaction

1. Under **Terminal**, click **Card present**. The Enter Card Present Transaction screen appears.



2. In the **Account** field, select the account configuration to use to process the transaction through ***Blackbaud Merchant Services***.

   Note: If an account configuration does not appear as an option, Blackbaud may not have been able to verify a disbursement account at your organization. For assistance, please contact Blackbaud Support.

3. In the **Amount** field, enter the amount of the transaction to process.
4. In the **Comment** field, you can enter any additional information about the transaction.

Tip: If you use a browser other than Microsoft *Internet Explorer* to access the web portal, you must click in a text field such as the **Amount** or **Comment** field before you swipe the credit card to successfully process its information.

5. To enter the credit card information through a card swipe reader, click **Enter Card Info** and swipe the credit card. Under **Account holder**, the information from the card swipe reader appears. The web portal automatically submits the transaction to ***Blackbaud Merchant Services***.

   Tip: Some credit cards issued in the United Kingdom, such as Solo, Switch, and Maestro, require an issue date and issue number. Enter this information in the **Valid from** and **Issue number** fields. Typically, the issue number is "01" unless the cardholder previously had the card replaced.

6. Click **Submit**. The web portal submits the transaction to ***Blackbaud Merchant Services***.

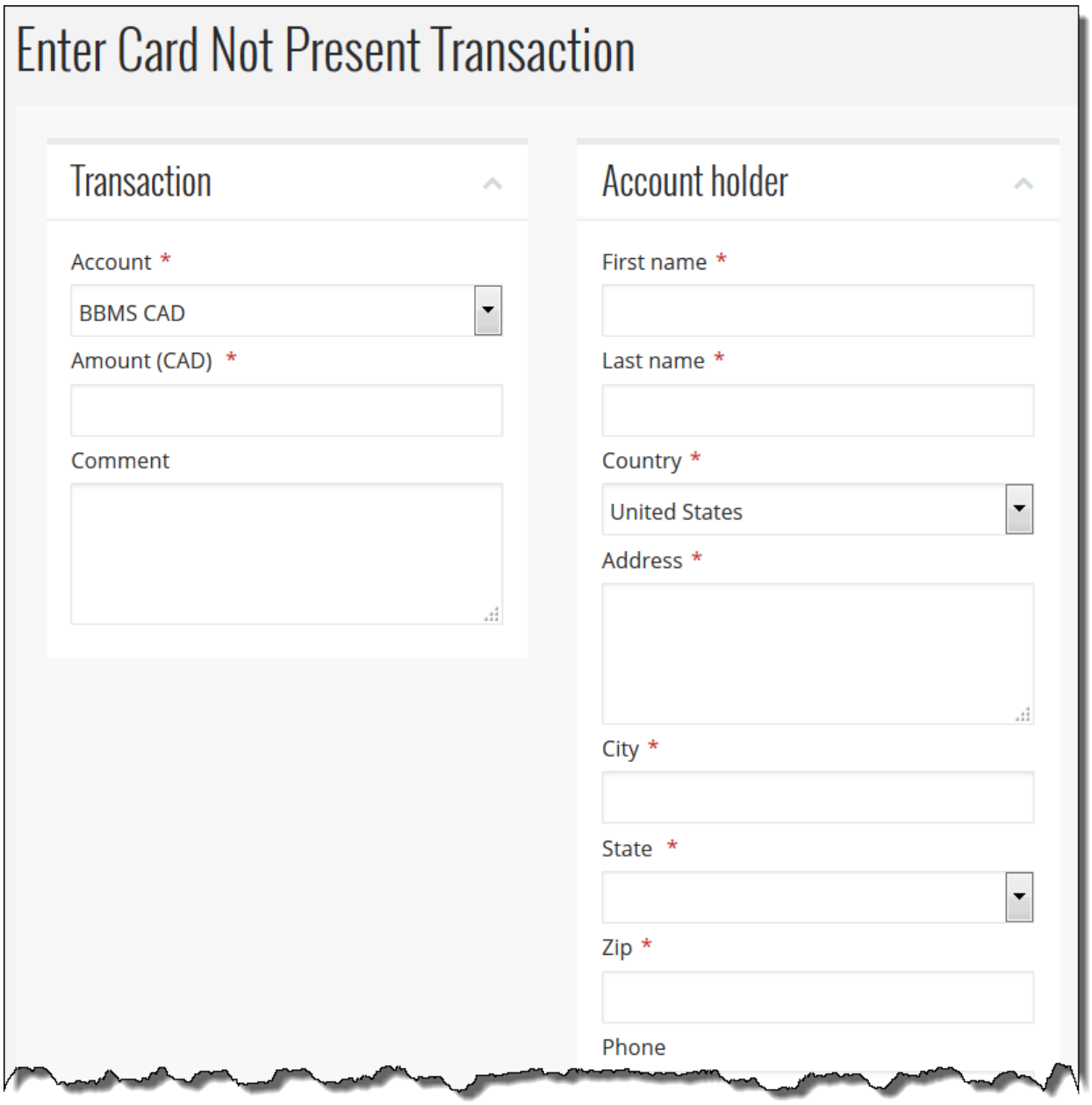
Card-Not-Present Transactions

You can manually submit card-not-present transactions to ***Blackbaud Merchant Services*** directly through the web portal.

Warning: When you process a transaction directly through the web portal, no corresponding record of the transaction appears in the database of your Blackbaud program. To maintain a record of the transaction, such as to include in reports on giving or revenue activity, we recommend you enter and process transactions through your Blackbaud program.

Submit a card-not-present transaction

1. Under **Terminal**, click **Card not present**. The Enter Card Not Present Transaction screen appears.



2. In the **Account** field, select the account configuration to use to process the transaction through ***Blackbaud Merchant Services***.

   Note: If an account configuration does not appear as an option, Blackbaud may not have been able to verify a disbursement account at your organization. For assistance, please contact Blackbaud Support.

3. In the **Amount** field, enter the amount of the transaction to process.
4. In the **Comment** field, enter any additional information about the transaction.
5. Under **Account holder**, enter the name, address, and contact information of the card holder.

6. Under **Card information**, enter the information from the credit card such as card holder name, primary account number, card security code, and expiration date.

   Note: Some credit cards issued in the United Kingdom, such as Solo, Switch, and Maestro, require an issue date and issue number. Enter this information in the **Valid from** and **Issue number** fields. Typically, the issue number is "01" unless the cardholder previously had the card replaced.

7. Click **Enter Card Info**. In the pop-up screen, enter the card information.
8. Click **Submit**. The web portal submits the transaction to ***Blackbaud Merchant Services***.

Transactions

Through the web portal, you can search for and manage transactions. You can also review suspect transactions and export transactions as needed.

Transaction Search

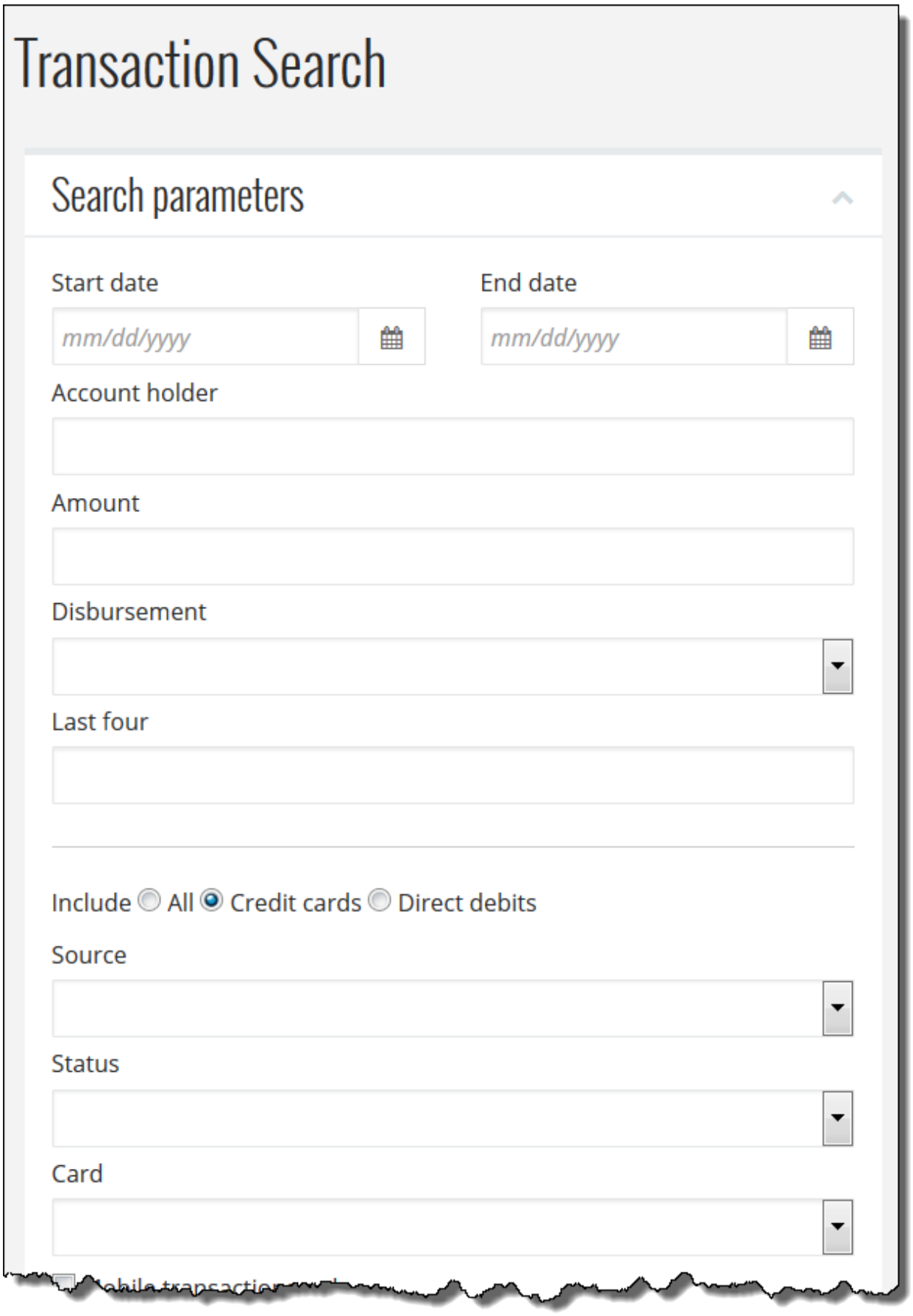
From the web portal, you can access a record of each credit card or direct debit transaction processed by ***Blackbaud Merchant Services*** for your organization's account. You can also initiate a refund of a transaction to the account holder as necessary. To view a transaction record or initiate a refund, you can use criteria such as payment information, amount, or transaction date to search ***Blackbaud Merchant Services*** for the transaction. When you search for a transaction, you can make the search broad or specific, depending on the criteria you select. To get the results you need, we recommend you be selective in your search criteria and use detailed information such as account holder name and amount.

Tip: To receive notification of when ***Blackbaud Merchant Services*** approves a live transaction for your account, you can use Really Simple Syndication (RSS) to subscribe to the Recent transactions feed through your web browser or an RSS reader that supports authenticated feeds. To subscribe to the RSS feed, click the RSS icon on the Transaction Search page. When you subscribe to the feed, you can view the transactions approved during the past 14 days, up to the cache limit of the RSS reader. You can also subscribe to email notifications. For more information, see Email Notifications on page 4.

Tip: To search for a credit card transaction submitted to ***Blackbaud Merchant Services*** through ***Blackbaud MobilePay***, include only credit cards and then select **Mobile transactions only**.

Search for a transaction

1. Under **Transactions**, click **Transaction search**. The Transaction Search page appears.


Transaction Search
Search parameters
Start date
mm/dd/yyyy
End date
mm/dd/yyyy
Account holder
Amount
Disbursement
Last four
Include All Credit cards Direct debits
Source
Status
Card

2. Use the **Start date** and **End date** fields to enter the date range within which ***Blackbaud Merchant Services*** processed the transaction.
3. In the **Account holder** field, enter the name of the account holder as it appears on the credit card or bank account of the transaction.
4. In the **Amount** field, enter the total amount of the transaction.
5. In the **Disbursement** field, select the disbursement associated with the transaction. To search for a transaction that has not yet been disbursed, select Undisbursed.
6. In the **Last four** field, enter the last four digits of the bank account number or the primary account number (PAN) of the credit card.
7. For **Include**, select whether to include all transactions or only credit card or direct debit transactions.
8. In the **Source** field, select how you submitted the transaction to ***Blackbaud Merchant Services***. For example, you can select whether to include only transactions submitted through a transaction batch or as refunds.
    - If you select **Credit cards**, you can also select to include only card-not-present or card-present transactions, or chargeback requests. To view a transaction submitted through ***Blackbaud MobilePay***, select **Mobile transactions only**.
    - If you select **Direct debits**, you can also select to include refunds, direct debit returns, or a direct debit batch.
9. In the **Status** field, select the processing result of the transaction, such as Approved or Processing Error.
10. If you select **Credit cards**, select the type of credit card used for the transaction, such as Visa or Mastercard.
11. If you select **Direct debits**, enter the check number of the transaction.
12. To view a transaction submitted through an account configuration set to Test mode, select **Include test transactions**.
13. Click **Search**. A grid displays the transactions that meet the criteria entered.

    Tip: In the search results, suspect transactions appear with an exclamation mark (!) and an action of Suspect.

    From the grid, you can view detail information about a transaction, refund a transaction to the account holder, or export the search results.

    - To see a transaction record, click the ellipsis next to the transaction you want to see and click **Details**.
    - To enter new search criteria, such as if the search did not return the transaction you wanted, click **Return to search** on the action bar. The criteria fields appear so you can refine the search as necessary.
    - To view detail information about a transaction in the search results, select the transaction in the grid and click **Details** on the action bar. For a refund or chargeback transaction,

select the transaction in the grid and, on the action bar, click **Details** and select **Transaction** or **Reference transaction**. The record of the transaction appears. For information about the items on the record, see Transaction Record on page 16.

- To refund a transaction in the search results to the account holder, select the transaction in the grid and click **Refund** on the action bar. For information about how to refund a transaction, see Refund a Transaction on page 18.
- To export the search results to a comma-separated values (*.csv) file or a Microsoft *Excel* (*.xls) spreadsheet, click **Export** on the action bar and select the output format for the export file.

  For information about the details included in an export file, see Transaction Export on page 19.

Transaction Record

Blackbaud Merchant Services maintains a record of each transaction processed for your organization. Through the web portal, you can search for and access a transaction record to view detail information such as the credit card or bank account, donor IP address, processing rate and fee, and gateway results associated with the transaction. To access a transaction record, you can search ***Blackbaud Merchant Services*** for the transaction. For information about how to search for a transaction, see Transaction Search on page 13.

Under **Transaction**, you can view information about the credit card or bank account used for the transaction, including account holder name, the last four digits of the account number, expiration date, and billing address. You can view detail information about the transaction such as the program used to submit the transaction to ***Blackbaud Merchant Services***, the rate and fee applied to the transaction, its net amount, and whether the transaction can be disbursed.

Tip: To search for a transaction submitted to ***Blackbaud Merchant Services*** through a mobile application such as ***Blackbaud MobilePay***, include only credit card transactions and then select **Mobile transactions only**. From the record of a mobile transaction, you can click **View mobile signature** to see the signature captured from the card holder at the time of the transaction. You can also resend the email acknowledgement sent to the card holder for a mobile transaction. For information about how to resend an email acknowledgement, see Resend an Email Acknowledgement on page 18.

Under **Result details**, you can view the processing result for the transaction, such as whether it was approved. You can also view the code and reference number associated with the result. For information about the processing results, see Transaction Results on page 17.

- With fraud management enabled, you can view details about the risk assessment of a card-not-present transaction from the record of the transaction. For information about fraud management details, see Fraud Details on page 18.
- To view why and when a suspect transaction is marked as suspect, click **Details** in the **Suspect Transaction** field. If you determine that the transaction is valid and incorrectly marked as suspect, you can accept it so it returns to ***Blackbaud Merchant Services*** for disbursement during the next disbursement cycle. To accept a transaction marked as suspect, click **Accept** and then click **Yes** when a confirmation message appears. For more information, see Suspect

Transactions on page 19.

> ***Note:*** From the Suspect Transactions page, you can access the record of a suspect transaction, such as to view detail information. On the record of the transaction, an explanation of why ***Blackbaud Merchant Services*** flagged the transaction as suspect appears under **Suspect transaction details**. If you determine the transaction to be valid, click **Accept**.

Under **Related Transactions**, you can view any associated refund transactions. From a transaction record, you can click **Refund** to return the transaction to the card holder if necessary. For information about how to refund a transaction, see Refund a Transaction on page 18.

From *Chargebacks*, you can access the record of a chargeback transaction. Under **Chargeback details**, you can view the reason for the chargeback and the disputed amount of the transaction. For a challenged chargeback, you can also view the date of the challenge and any files or notes added in support of the challenge. For information about how to challenge a chargeback pending review, see Challenge a Chargeback on page 27. For information about the chargeback reason, see Chargeback Reasons on page 25.

For adjustments, you can see whether the transaction is a tax withholding or a fee refund on the **Type** field.

Transaction Results

On a transaction record, the **Result** field displays the processing result for the transaction. The table below explains the results possible for a transaction.

Result	Description
Gateway Processing	***Blackbaud Merchant Services*** is currently processing the transaction. If you submit a transaction batch, this result appears for its transactions until ***Blackbaud Merchant Services*** completely processes all transactions in the batch. Depending on the size of the batch, it may take some time to process the transactions.
Gateway Decline	***Blackbaud Merchant Services*** declined the transaction, such as due to insufficient funds, incomplete information, or a processing error.
Approved	***Blackbaud Merchant Services*** successfully processed the transaction.
Pending	For a direct debit transaction, ***Blackbaud Merchant Services*** is currently awaiting authorization from the bank. Typically, this is the next business day after the transaction.
Validation error	There was an error at the validation stage so the transaction was not completed.
Processing error	There was an error at the processing stage so the transaction was not completed.
Not processed	The transaction was not processed for another reason.

Fraud Details

With fraud management enabled, you can view details about the risk assessment of a card-not-present transaction from the record of the transaction. To view the fraud details, click **Details** in the **Fraud management** field under **Result details**. On the Fraud Details screen, you can view the risk score assigned the card-not-present transaction, the risk score threshold set when the transaction processed, and whether the transaction passed the various risk factors such as anonymous proxies and account velocity.

Note: If your organization does not enable account velocity screening, the message "Not Processed" appears in the **Velocity** field.

Refund a Transaction

From the web portal, you can refund an approved credit card or direct debit transaction to the account holder as necessary.

- For a credit card transaction, you can refund all or part of the transaction amount. The refund amount cannot exceed the amount of the transaction that remains after any additional refunds.
- For a direct debit transaction, you must refund the full transaction amount.

  Note: To prevent refunds for declined transactions, ***Blackbaud Merchant Services*** automatically holds refunds issued for direct debit transactions until five business days after the date of the original transaction. ***Blackbaud Merchant Services*** also automatically refunds any direct debit transactions that are approved but then returned by the bank.

To refund a transaction, open its record or select the transaction in search results or on the Suspect Transactions tab on the home page, and then click **Refund**. On the Refund transaction screen, enter the amount to refund to the account holder and click **Refund**.

Warning: When you refund a transaction through the web portal, no corresponding refund appears in the database of your Blackbaud program. To ensure accurate giving or revenue totals, we recommend you issue refunds through your Blackbaud program when applicable.

Resend an Email Acknowledgement

When you accept credit card transactions through the ***Blackbaud MobilePay*** mobile application, the application automatically sends the card holder an acknowledgement for the transaction as an email message. If necessary, you can send the acknowledgement to the cardholder again from the portal, such as to correct the recipient email address.

Tip: To search for a transaction submitted to ***Blackbaud Merchant Services*** through ***Blackbaud MobilePay***, select "Card present" in the **Source** field and then select **Mobile transactions only** on the Transaction Search page.

On the record of the mobile transaction, click **Resend acknowledgement**. On the Resend acknowledgement screen, the recipient email address of the original acknowledgement appears, along with the "Reply to" email address and default subject line configured for email acknowledgements. Edit this information as necessary and click **Send acknowledgement**.

Note: For information about how to configure the default information to appear in email acknowledgements created by ***Blackbaud Merchant Services***, see Email Acknowledgement Settings on page 37.

Suspect Transactions

Blackbaud Merchant Services automatically flags transactions as suspect when they meet specific criteria, such as:

- A questionable IP address
- A transaction amount that exceeds $10,000
- Multiple identical transactions from the same credit card within a short amount of time

Blackbaud Merchant Services disburses funds from suspect transactions, but flags them for your review. When you log on to the web portal, the **Message Center** on the home page displays whether suspect transactions await review. To view and manage any transactions flagged as suspect, on the home page, click the **Suspect transactions** tab.

The grid displays information about the suspect transactions, including the credit card used and the reason ***Blackbaud Merchant Services*** flagged the transaction as suspect. From the grid, you can manage each suspect transaction.

- If you determine that a suspect transaction is a valid transaction, you can accept the transaction. To accept a transaction, select it in the grid and click **Accept** on the action bar.
- If you determine that a suspect transaction is fraudulent, you can refund the transaction to the card holder. To refund a transaction, select it in the grid and click **Refund** on the action bar. For information about how to refund a transaction, see Refund a Transaction on page 18.

To help determine whether to accept or refund a suspect transaction, you can access detail information about the transaction. In the grid, select the transaction to view and click **Details** on the action bar. The record of the suspect transaction appears. For information about the items on the record, see Transaction Record on page 16.

Tip: To know when ***Blackbaud Merchant Services*** posts a suspect transaction to your account, set up email notifications for suspect transactions and large suspect transactions. For information, see Email Notifications on page 4.

Transaction Export

From the Transaction Search screen, you can click **Export** to export information about the transactions included in the search results to a comma-separated values (*.csv) file or a Microsoft *Excel* (*.xls) spreadsheet. The table below explains the fields included in the export file.

Export field	Description
Transaction ID	This field provides the unique identifier that ***Blackbaud Merchant Services*** assigned the transaction.

Export field	Description
Date	This field provides the date ***Blackbaud Merchant Services*** processed the transaction.
Source	This field provides how ***Blackbaud Merchant Services*** received the transaction, such as card not present, refund, or chargeback.
Account holder	This field provides the account holder name entered for the transaction's credit card or bank account.
Account type	This field provides the type of credit card or payment method used for the transaction, such as Visa, MasterCard, or Direct debit.
Last 4	This field provides the last four digits of the credit card or bank account number processed for the transaction. For security, the other digits of the card number appear as asterisks.
Expiry	For a credit card transaction, this field provides the expiration date of the card.
Currency	This field provides the currency type of the transaction, such as USD or CAD.
Gross amount	This field provides the total amount processed for the transaction, including any processing fees.
Result	This field provides the processing result for the transaction, such as whether it was approved. For information about processing results, see Transaction Results on page 17.
Fees	This field provides the total amount of processing fees assessed for the transaction.
Net amount	This field provides the amount disbursed for the transaction. Typically, this amount is the gross amount less any processing fees.
Comment	This field provides any additional information entered about the transaction.
Country	This field provides the country of the transaction's billing address.
Address	This field provides the street address of the transaction's billing address.
City	This field provides the city of the transaction's billing address.
State	This field provides the state or province of the transaction's billing address.
ZIP Code	This field provides the postal code of the transaction's billing address.
Email	This field provides an email address associated with the account holder, such as for the email acknowledgement of a mobile transaction.
Phone	This field provides a phone number associated with the account holder.
Risk score	For a card-not-present transaction, this field provides the risk score that ***Blackbaud Merchant Services*** assigned the transaction. For information about how to enable and configure fraud management, see Fraud Management on page 36.

Export field	Description
Risk threshold	For a card-not-present transaction, this field provides the maximum risk score allowed when ***Blackbaud Merchant Services*** processed the transaction. For information about how to set this threshold, see Fraud Management on page 36.
Anonymous proxy	For a card-not-present transaction, this field provides whether the transaction passed the screening for transactions from anonymous proxies. If your organization does not select to reject transactions from anonymous proxies, "Not Processed" appears. For information about this screening, see Fraud Management on page 36.
High risk country	For a card-not-present transaction, this field provides whether the transaction passed the screening for transactions from countries with a high risk of fraudulent activity. If your organization does not select to reject transactions from high risk countries, "Not Processed" appears. For information about this screening, see Fraud Management on page 36.
BIN and IP country	For a card-not-present transaction, this field provides whether the transaction passed the verification that the country of the Bank Identification Number (BIN) matches the country of the billing address. If your organization does not select to verify the countries match, "Not Processed" appears. For information about this screening, see Fraud Management on page 36.
Velocity	For a card-not-present transaction, this field provides whether the transaction passed the screening for account velocity, or the rate of transactions from the same credit card number within a short amount of time. For information about this screening, see Fraud Management on page 36.
Terminal type	For a card-present transaction, this field provides where the transaction was accepted, such as a ***Blackbaud MobilePay*** device or a self-service ticket kiosk.
Check number	For a direct debit transaction, this field provides the number entered for the online check.
Pending date	For a direct debit transaction, this field provides the expected date of the bank's authorization of the transaction. Typically, this is the next business day after the transaction.
Mobile device security code	For a ***Blackbaud MobilePay*** transaction, this field provides the security code assigned the mobile device used to accept and submit the transaction. For information about mobile devices, see Mobile Devices on page 46.
Screened for fraud	For a card-not-present transaction, this field indicates whether the premium Fraud Management filters checked the transaction. For information about this screening, see Fraud Management on page 36.
Application	This field provides which Blackbaud program submitted the transaction for processing.

Batch Search

From the web portal, you can search for and view a specific batch of transactions processed by ***Blackbaud Merchant Services*** for your organization. From a batch, you can access a specific transaction or initiate a refund of a transaction to the account holder as necessary. To view a transaction batch, you can use the date range of when your organization submitted the batch to ***Blackbaud Merchant Services*** and select whether to include batches with test transactions or only completed batches. When you search for a batch, you can make the search broad or specific, depending on the criteria you select. To get the results you need, we recommend you be selective in your search criteria.

Warning: The transaction batch search does not apply to transactions processed through ***eTapestry***, ***Luminate CRM***, or ***Luminate Online***. Instead, use the transaction search to find a transaction through the portal. For information about transaction search, see Transaction Search on page 13.

Search for a transaction batch

1. Under **Transactions**, click **Batch search**. The Batch Search screen appears.
2. Enter the date range in which your organization submitted the batch to ***Blackbaud Merchant Services***.
3. In the **Type** field, select whether to restrict the search to batches that contain only credit card or direct debit transactions or refunds.
4. To restrict the search to only completed batches, select **Completed batches only**.
5. Select whether to include batches with test transactions in the search.
6. Click **Search**. The batches that meet the selected criteria appear.

   Tip: To enter new search criteria, such as if the search did not return the batch you wanted, click **Return to search**. The criteria fields appear so you can refine the search as necessary.
7. In the grid, click the ellipsis next to the batch you want to view and click **Details**. A grid displays the transactions included in the selected batch.
   - To return to the search results, such as to view the transactions of another batch from the same date range, click **Return to batch**. A grid displays the batches that meet the criteria entered.
   - To view detail information about a transaction in the search results, select the transaction and click **Details**. The record of the transaction appears. For information about the items on the record, see Transaction Record on page 16.
   - To refresh the status of transaction with a status of Gateway processing or Gateway processing complete, select the transaction in the grid and click **Update status**.
   - To view detail information about a refund or chargeback transaction in the search results, select the transaction in the grid and, on the action bar, click **Details** and select **Transaction** or **Reference transaction**. The record of the transaction appears. For information about the items on the record, see Transaction Record on page 16.
   - To refund a transaction in the search results to the card holder, select the transaction in the

grid and click **Refund**. For information about how to refund a transaction, see Refund a Transaction on page 18.

Chargebacks and Direct Debit Returns

At times, account holders may dispute the validity of transactions with the credit card company or bank, such as if the credit card is reported stolen or the account holder does not recognize the transaction. When this occurs, your account may receive a request for a chargeback or direct debit return.

- When the account holder disputes a credit card transaction, the credit card company issues a chargeback request to ***Blackbaud Merchant Services***. In some cases, such as when the credit card company determines fraudulent activity, ***Blackbaud Merchant Services*** must automatically refund the transaction to the card holder. In other cases, ***Blackbaud Merchant Services*** may automatically challenge the chargeback, such as if your organization has already issued a refund for the disputed transaction. Other types of chargebacks, such as when the card holder does not recognize a transaction, require attention from your organization.

  Tip: When you log on to the web portal, the **Message Center** on the home page displays whether any chargeback transactions require your attention.

- When the account holder disputes a previously approved direct debit transaction, or the bank cannot authorize a direct debit transaction due to insufficient funds or a closed account, the bank issues a direct debit return. ***Blackbaud Merchant Services*** automatically refunds returned direct debit transactions to the account holder.

From the web portal, you can view these transactions and manage any chargeback requests that require input from your organization, such as any collateral to determine the validity of a disputed transaction.

Chargeback Reasons

When a card holder disputes the validity of a transaction with their credit card company, the credit card company issues a chargeback request to ***Blackbaud Merchant Services***. In some cases, ***Blackbaud Merchant Services*** must automatically refund the transaction to the card holder. In other cases, you can challenge a chargeback request based on the validity of the transaction. For information about how to challenge a chargeback request, see Challenge a Chargeback on page 27.

The following table explains the collateral required to dispute each reason of chargeback request.

Chargeback reason	Collateral
Compliance	This chargeback request indicates a transaction that did not comply with your card acceptance agreement with the credit card company or is otherwise uncollectible. You cannot challenge this type of chargeback. ***Blackbaud Merchant Services*** must refund the transaction to the card holder.
Fraud transaction—unauthorized	This chargeback request indicates a fraudulent or unauthorized transaction, such as through stolen credit card information. You cannot challenge this type of chargeback. ***Blackbaud Merchant Services*** must refund the transaction to the card holder.
Credit previously issued	This chargeback request indicates the card holder was issued a duplicate credit for a transaction. If you have already issued a refund for the duplicate credit, provide a screen capture of a record of the processed refund to dispute the request.
Canceled recurring transaction	This chargeback request indicates the card holder reports the transaction as toward a canceled commitment such as a pledge or recurring gift. To dispute the request, provide a screen capture of a record of the commitment.
Transaction not recognized	This chargeback request indicates the card holder does not recognize the transaction. To dispute the request, provide a screen capture of a record of the transaction.
Credit not processed	This chargeback request indicates the card holder did not receive a requested refund for a transaction. To dispute the request, provide documentation that explains why the refund was denied.
Duplicate transaction (processing)	This chargeback request indicates the card holder believes a transaction to be a duplicate of another transaction. To dispute the request, provide screen captures of records of the valid transactions presumed to be duplicates.
Non-receipt of merchandise	This chargeback request indicates the card holder did not receive the product purchased with the transaction. To dispute the request, provide documentation as evidence the card holder received the product, such as delivery confirmation.
Not as described	This chargeback request indicates the card holder received a product or service different from that purchased with the transaction. To dispute the request, provide documentation to describe the product or service the card holder received.
Services not rendered	This chargeback request indicates the card holder did not receive the service purchased with the transaction. To dispute the request, provide documentation as evidence that the card holder agreed to and used the service.
Other	For card-present transactions processed by American Express, provide documentation as evidence of signed support such as an endorsed acknowledgement. For all other transactions, contact chargebacks@blackbaud.com for information about how to dispute the request.

Chargebacks Pending Review

To view and manage open chargeback requests, from the home page click **Chargebacks pending review**.

Tip: To receive notification of when ***Blackbaud Merchant Services*** posts a pending chargeback to your account, you can use Really Simple Syndication (RSS) to subscribe to the grid as a feed through your web browser or an RSS reader that supports authenticated feeds. To subscribe to the RSS feed, click the RSS icon.

The grid displays information about the chargebacks, including the original, disputed transaction and the reason the card holder disputes the transaction. From the grid, you can select whether to challenge or accept each chargeback request.

- If you determine that a transaction disputed by a chargeback is valid, you can challenge the chargeback request. For information about how to challenge a chargeback, see Challenge a Chargeback on page 27.
- If you determine that a transaction disputed by a chargeback is not a valid transaction, you can accept the chargeback request to refund the disputed amount to the credit card account. To accept a chargeback, click the ellipsis to the left of the chargeback and click **Accept**.

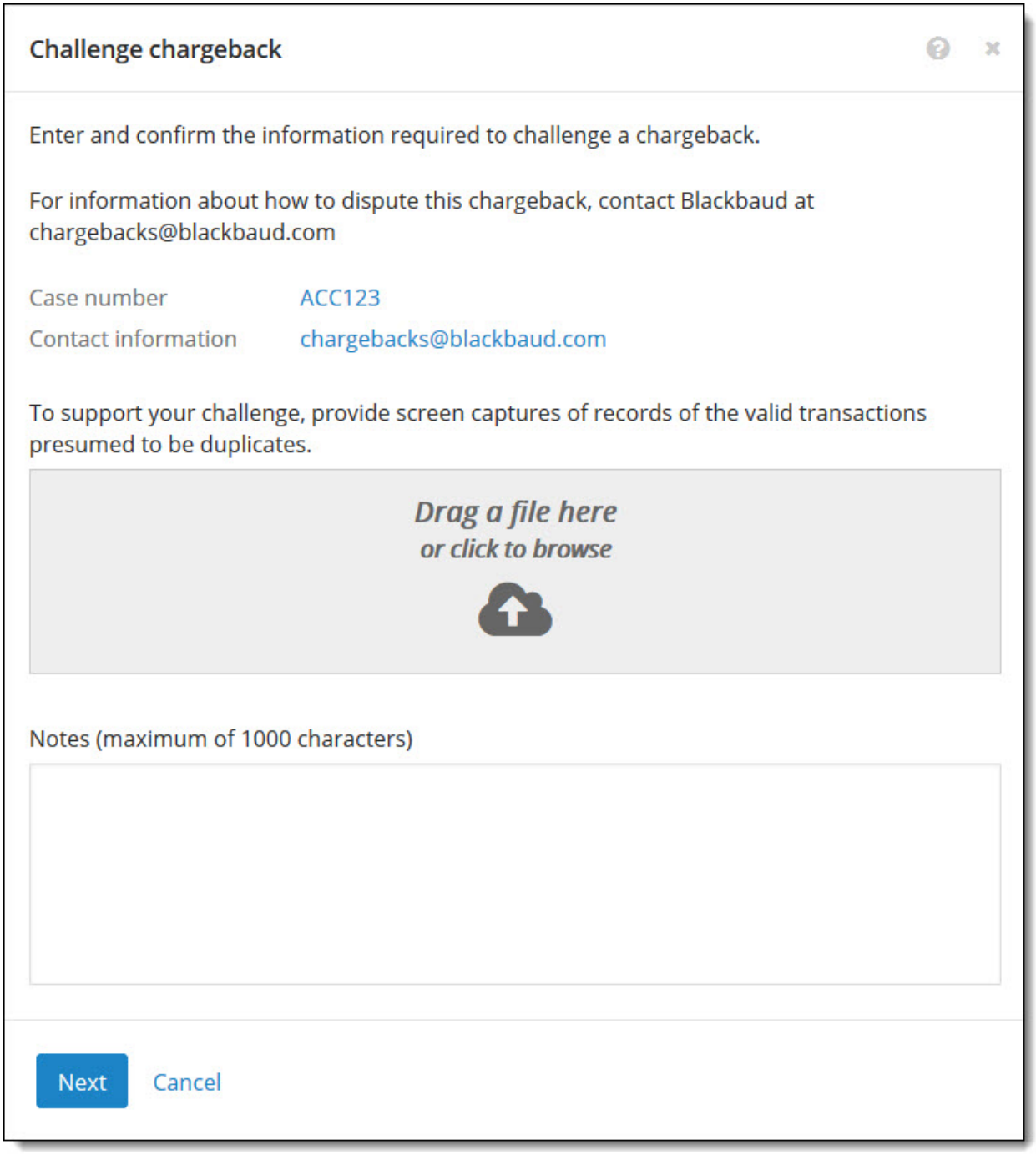
To help determine whether to challenge or accept a chargeback request, you can access detail information about the chargeback. In the grid, click the ellipsis to the left of the chargeback and click **Details** on the action bar. The record of the chargeback appears. For information about the items on the record, see Transaction Record on page 16.

Challenge a Chargeback

If you determine that a transaction disputed by a chargeback is valid, you can challenge the chargeback request from the Chargebacks Pending Review page. When you challenge a chargeback request, you must provide collateral to support the dispute, such as a screenshot of the transaction record within your Blackbaud program. For information about the collateral required for each type of chargeback request, see Chargeback Reasons on page 25.

Challenge a chargeback request

1. On the home page, click **Chargebacks pending review**.
2. For the chargeback you want to challenge, click the ellipsis next to the chargeback you want to challenge and click **Challenge**. The Challenge chargeback screen appears and displays the case number and contact information associated with the chargeback.



3. Browse to the files to use as evidence in support of your challenge. The file must be in a Joint Photographics Expert Group (*.jpg or *.jpeg) format, portable network graphics (*.png) format, graphics interchange format (*.gif), portable document format (*.pdf), text (*.txt) format, Microsoft *Word* document (*.doc), or *Office* Open XML document (*.docx) format.

   To remove all uploaded files, click **Clear all files**.

4. In the **Notes** field, enter any additional information about the chargeback challenge.

5. Click **Next**. A summary page appears.
6. Review the information entered about the chargeback and its challenge. To edit or correct any information, click **Back** to the previous page.
7. Click **Finish**.

Chargebacks Under Dispute

To view and manage challenged chargeback requests, on the home page, click **Chargebacks under dispute**.

The grid displays information about the challenged chargebacks, including the original, disputed transaction and the reason the card holder disputes the transaction. To view additional information about a disputed chargeback request, click the ellipsis to the left of the chargeback and click **Details** on the action bar. The record of the chargeback appears. For information about the items on the record, see Transaction Record on page 16.

Resolved Chargebacks and Direct Debit Returns

To view and manage accepted or successfully challenged and closed chargebacks and direct debit transactions returned due to an account holder dispute, on the home page, click **Chargebacks resolved**.

The grid displays information about the resolved chargebacks and returns, including the original, disputed transaction; the reason for the chargeback or return; and the resolution to the dispute. To view additional information about a chargeback request or direct debit return, click the ellipsis to the left of the chargeback and click **Details** to open its record. For information about the items on the record, see Transaction Record on page 16.

Reports

From the web portal, you can access reports to view information about your disbursements and the credit card transactions processed by ***Blackbaud Merchant Services***.

Disbursement Report

From the web portal, you can access a summary or detailed report of your organization's activity for each disbursement period, such as to reconcile with your bank account. On either report, you can view information about the amount of the disbursement for the period and into which account Blackbaud deposits the disbursement. For the disbursement, you can view its transactions and reversals by source, such as through card-not-present transactions or a transaction batch from your Blackbaud product.

- On the Disbursement Summary Report, for each source, you can view a breakdown of activity by credit card type, such as MasterCard and Visa, and the fees associated with each card type. You can also view information about the fee schedules associated with the transactions included in the disbursement.
- On the Disbursement Detailed Report, for each source, you can view each transaction processed and the fees associated with each transaction.

To view a disbursement report, click **Disbursement** under **Reports**, select its disbursement date, and select whether to generate it as a portable document file (*.pdf) or Microsoft *Excel* spreadsheet (*.xls).

Tip: To receive alerts of when ***Blackbaud Merchant Services*** posts a disbursement to your account, you can use Really Simple Syndication (RSS) to subscribe to the Disbursement Reports page as a feed through your web browser or RSS reader. To subscribe to the RSS feed, click the RSS icon. You can also subscribe to email notifications. For more information, see Email Notifications on page 4.

Note: For disbursement accounts held at most major banks, funds are direct-deposited on the fifth business day after the last day of the disbursement cycle. Funds may take slightly longer to deposit into accounts held at smaller banks, savings and loans, and credit unions.

Daily Transactions Report

To view a list of the credit card and direct debit transactions processed by ***Blackbaud Merchant Services*** for your account on a specific date, you can generate the Daily Transactions Report. For each transaction, you can view its source, its gross and net amounts, any associated fees, information about the credit card or bank account used, and its result.

To generate the Daily Transactions report, click **Daily transactions** under **Reports**. The report page appears. Select the criteria and grouping of the transactions to include in the report and click **Run Report**.

- In the **Date** field, select the date or date range for which to view transactions. If you select Specific date, select the date of the transactions to view.
- In the **Result** field, select the result of the transactions to view such as Approved. To view all transactions for the client on the selected date, regardless of result, leave the **Result** field blank.
- In the **Group by** field, select whether to group the transactions in the report by date or account type.

Account Management

From the web portal, you can manage your organization's account with ***Blackbaud Merchant Services***. Under **Account Management**, you can manage information about the bank account where you receive disbursements and maintain contact information for your organization. You can add and manage the account configurations your organization uses to process transactions through ***Blackbaud Merchant Services***, set up fraud management for card-not-present transactions, and manage the users at your organization who access the portal and their roles. You can also manage email acknowledgement settings and your mobile devices.

Disbursement Account Information

From the web portal, you can view and manage information about the accounts through which you receive disbursements from ***Blackbaud Merchant Services***. You must use a separate bank account for each type of currency you process.

Note: To process payments in a specific currency, your organization must have a presence in the country where the currency is disbursed, including a local bank account in that country.

To manage your bank account information through the web portal, under **Account Management**, click **General Settings**. The General Settings page appears and displays the accounts your organization uses with ***Blackbaud Merchant Services***.

Warning: When you add or edit a bank account, ***Blackbaud Merchant Services*** suspends its disbursements pending verification of the account. To verify the account, you must provide the required documentation to authenticate your organization and its mission.

Note: To process in Canadian dollars (CAD), payment industry regulations require information about members of your Board of Directors to verify your organization. For information about how to manage a list of your board members, see Board of Directors Information on page 34.

Warning: Before you delete a bank account, verify there are no pending disbursements scheduled for the account.

From the grid, you can manage your account information as necessary.

Edit bank account information

Note: If Blackbaud has declined an account, such as if it still needs verification, you cannot edit its information. To verify the account, you must provide the required documentation to authenticate your organization and its mission.

1. Under **Account Management**, click **General Settings**. The General Settings page appears.
2. In the Account Information section, click **Edit account**. The Edit an Account screen appears.
3. Edit the account information as necessary.

   Note: For information about how to update information about your Board of Directors for a Canadian dollar (CAD) account, see Board of Directors Information on page 34.
4. Click **Save**. You return to the General Settings page.

   Note: If Blackbaud has declined an account, such as if it still needs verification, you cannot edit it. To verify the account, you must provide the required documentation to authenticate your organization and its mission.

Board of Directors Information

To process in Canadian dollars (CAD), payment industry regulations require information about members of your Board of Directors to verify your organization. To manage a list of your board members, click **Review/Edit List** when you add or edit disbursement information for a CAD account.

Note: Blackbaud Merchant Services automatically retrieves any known information about your board members from ***Nonprofit Central*** based on your tax ID.

Under **Board of Directors**, you can add and manage board member information as necessary.

- To save information about a new member, click **Add director**, enter their first and last name, and click **Save**.
- To change information about a member, such as to correct a typographical error, select their name, click **Edit**, update their first or last name, and click **Save**.
- To remove a member from the list, select their name and click **Delete**. When a message appears to ask whether to delete the member, click **Delete board member**.

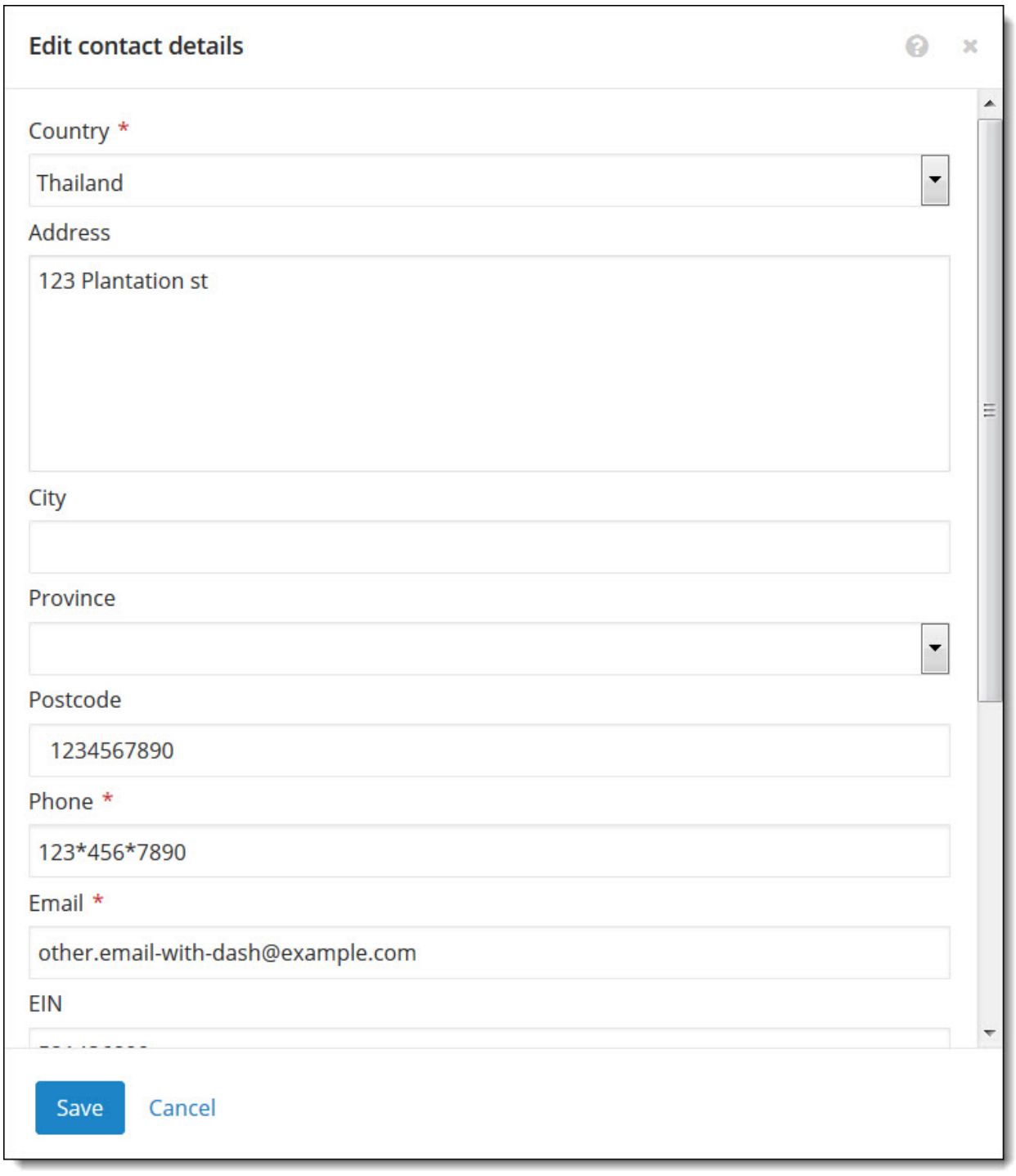
Contact Details

From the web portal, you can view and manage your organization's contact information. Blackbaud uses this information to contact your organization about your account, transactions, or disbursements. You can also manage the name and phone number that appear on credit card and bank statements for transactions your organization processes through ***Blackbaud Merchant Services***. Donors can use this information to contact your organization about a transaction.

To manage your contact information through the web portal, under **Account Management**, click **General Settings**. The General Settings page appears and displays your contact information. You can edit this information as necessary.

Edit contact information

1. Under **Account Management**, click **General Settings**. The General Settings page appears.
2. In the Contact details section, click **Edit contact details**. The Contact Details screen appears.



3. Edit the address and contact information as necessary.
4. If your address or disbursement account is in the United States, in the **EIN** field, enter your organization's Employer Identification Number (EIN). ***Blackbaud Merchant Services*** uses the EIN to report disbursement information to the Internal Revenue Service (IRS).

5. Under **Statement descriptors**, enter the name or abbreviation and phone number to appear on credit card and bank statements to identify transactions to your organization. In the **Name** field, you can enter up to 18 characters.
6. Click **Save**. You return to the General Settings page.

Fraud Management

Blackbaud Merchant Services automatically provides several fraud protection features, such as Card Security Code (CSC) check, Address Verification System (AVS), and Three-Domain Secure (3DS) authentication. ***Blackbaud Merchant Services*** also automatically flags transactions as suspect when they meet specific criteria, such as a questionable IP address.

To use additional fraud protection with card-not-present transactions, you can enable premium Fraud Management for your ***Blackbaud Merchant Services*** account. With premium Fraud Management enabled, ***Blackbaud Merchant Services*** evaluates many risk factors, including the IP address and country where a transaction originates and their relationship to the credit card and cardholder information, to determine the likelihood of a transaction being fraudulent. Based on this assessment, ***Blackbaud Merchant Services*** assigns a risk score from 0 to 100, with higher scores for transactions with a greater risk for fraud.

Note: To first enable premium Fraud Management, you must accept its terms and conditions. To view the terms and conditions before you set up a profile, click **View Terms and Conditions** on the Fraud Management page. This is a premium option, and your organization is charged a nominal fee for each transaction, including those processed in test mode. After you enable premium Fraud Management, you can turn it on and off at your convenience.

Tip: By default, we recommend you not accept transactions with a risk score greater than 35. To determine a maximum risk score that best meets the needs of your organization, we recommend you review your processed transactions and enter their average risk score as your maximum. You can view the risk score assigned a transaction from its record or in the results of a transaction search.

When you enable premium Fraud Management, you can enter the maximum risk score of the transactions to accept. You can also select whether to reject transactions based on the following risk factors, regardless of the risk score:

- **Anonymous proxies.** Scammers may use anonymous proxies to spoof IP addresses and hide their true locations to bypass geolocation controls. You can select whether to reject all transactions from anonymous proxies. ***Blackbaud Merchant Services*** will track information about the devices used to submit online transactions, to monitor for when a fraudster changes proxies while on a website or between visits to a donation page.
- **High-risk countries.** Some countries and regions have a high risk for fraudulent activity in regards to scams and stolen credit card usage. You can select whether to reject all transactions from high-risk countries such as Ghana, Vietnam, and Nigeria.
- **BIN country match.** The first six digits of a credit card number compose the Bank Identification Number (BIN) or Issuer Identification Number (IIN) and identify the institution that issued the card and its country of origin. You can select whether to reject all transactions when the countries of their credit cards' BIN do not match the countries of the cardholders' billing addresses.

- **Account velocity.** ***Blackbaud Merchant Services*** can automatically reject transactions based on account velocity, or the rate of transactions with the same credit card number, card type, and expiration date within a short amount of time.

Tip: While not all transactions with these risk factors are fraudulent, to help avoid chargeback requests and suspect transactions, we strongly recommend you reject all transactions from anonymous proxies or high-risk countries, transactions from countries other than their issuing banks', and transactions that exceed the account velocity.

To view your fraud settings through the web portal, click **General Settings** under **Account Management**. On the General Settings page, you can manage your fraud settings as necessary.

Edit the fraud management profile

1. Under **Account Management**, click **General Settings**. The General Settings page appears.
2. In the Fraud management options area, click **Edit fraud management options**. The Fraud Management screen appears.
3. To enable additional fraud protection for card-not-present transactions, select **Enable fraud management** and set the fraud settings.
   a. To determine the risk for fraud, ***Blackbaud Merchant Services*** evaluates many variables and assigns transactions with a greater risk for fraud with higher scores. Enter the maximum risk score to allow for accepted transactions.
   b. Select whether to reject all transactions from anonymous proxies, regardless of risk score. We recommend you select this option to help avoid fraudulent transactions from high-risk countries.
   c. Select whether to reject all transactions from IP addresses in high-risk countries, regardless of the risk score. While not all transactions from these areas are fraudulent, we recommend you select this option to help avoid chargeback requests and suspect transactions.
   d. Select whether to deny transactions when the country of the credit card's BIN does not match the country of the cardholder's billing address, regardless of the risk score. While not every transaction from a country other than its BIN is fraudulent, we recommend you select this option as many international credit cards do not support the Address Verification System (AVS).
   e. ***Blackbaud Merchant Services*** can deny transactions when they exceed a specific number of attempts within a short period of time. To apply this filter to card-not-present transactions, select **Enable account velocity screening**.
4. Click **Save**. You return to the General Settings page.

Email Acknowledgement Settings

From the web portal, you can set up information to appear in email acknowledgements created by ***Blackbaud Merchant Services***, such as for transactions through the ***Blackbaud MobilePay*** mobile application. When you configure your email settings, you specify how your organization's name appears as the sender and which email addresses to use as the sender and to receive replies and failure

notifications. You can also specify the subject lines to use by default and whether to always use them for email acknowledgements.

Edit email acknowledgement settings

1. Under **Account Management**, click **General Settings**. The General Settings page appears.
2. In the Email acknowledgement settings area, click **Edit email acknowledgement settings**. The Edit email acknowledgement settings screen appears.
3. In the **From display name** and **From address** fields, enter your organization's name and email address to appear as the sender of email acknowledgements.
4. In the **Reply to address** field, enter the email address to receive replies to email acknowledgements.
5. In the **Failure forwarding address** field, enter the email address to receive delivery failure notifications, such as for email bounces.
6. In the **Default subject** and **Default refund subject** fields, enter the default description to appear as the subject line of email acknowledgements for transactions and refunds.

   Tip: To include the amount of the transaction in the subject line, use "[total]" as a placeholder in the **Default acknowledgement subject** field. For example, enter "Thank you for your payment of [total]."

   To use this subject line with all email acknowledgements, regardless of the subject configured elsewhere such as ***Blackbaud MobilePay***, select **Always use default subject**.
7. Click **Save**. You return to the General Settings page.

Account Configurations

Through the web portal, you can configure your account with ***Blackbaud Merchant Services***. You can set up multiple configurations of your account, such as to process live and test transactions separately or to use separate configurations based on credit card type or fraud protection levels. Your organization must also set up a separate configuration for each type of currency you process. The account configurations that you add on this page appear as merchant accounts within *Terminal* and in your Blackbaud programs that interface with the ***Blackbaud Payment Service***.

To view and manage your account configurations through the web portal, click **General Settings** under **Account Management**. On the General Settings page, you can view the names and descriptions of your account configurations and the type of currency processed by each. You can also view whether a configuration uses a Card Security Code (CSC) check or Address Verification System (AVS) as fraud protection.

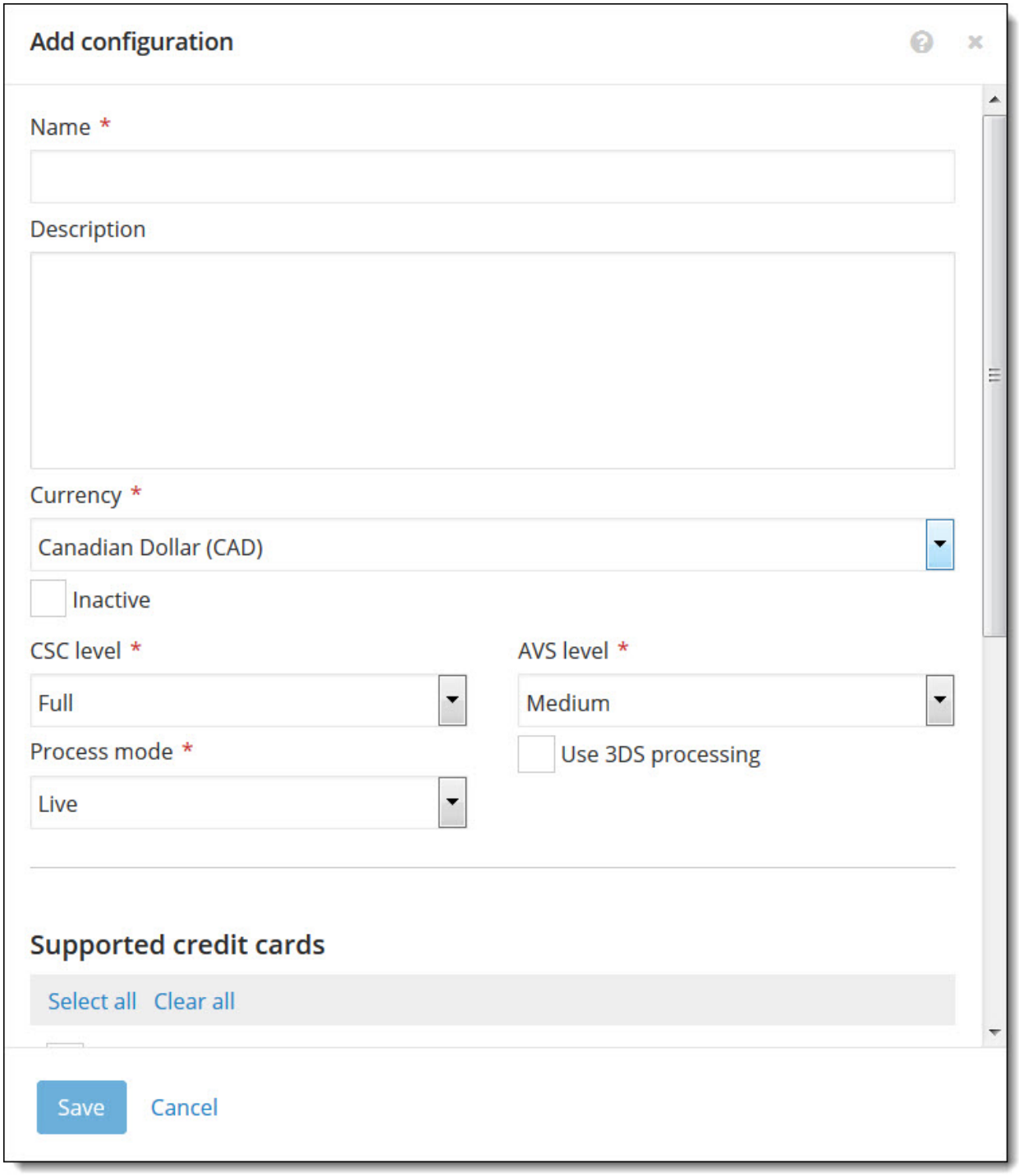
Tip: If your organization provisions multiple accounts with ***Blackbaud Merchant Services***, remember that each account has its own portal login credentials, and the portal displays only information about the account associated with the credentials used to log in. For analysis of all transactions processed through multiple ***Blackbaud Merchant Services*** accounts, use the Blackbaud program through which you submit transactions. For information about multiple ***Blackbaud Merchant Services*** accounts, see Manage Multiple Accounts on page 42.

From the General Settings page, you can manage your ***Blackbaud Merchant Services*** account configurations as necessary.

Warning: For ***eTapestry*** users, to ensure transactions process correctly, we recommend you not edit or delete the default configuration settings. Please contact ***eTapestry*** Support before you edit configuration settings.

Add account configurations

1. Under **Account Management**, click **General Settings**. The General Settings page appears.
2. In the Account configurations section, click **Add configuration**. The Add an account configuration screen appears.



3. Enter a unique name and description to help identify the account configuration.
4. In the **Currency** field, select the type of currency to process with the configuration.

Warning: To fully support a currency, you must also add a disbursement bank account to receive deposits of the currency type. For information about how to set up disbursement bank accounts, see Disbursement Account Information on page 33.

5. To set up the configuration but not make it available to process transactions, select **Inactive**.
6. In the **CSC level** field, select whether to use Card Security Code (CSC) checks with the configuration and at what level. For example, you may select to use CSC to process card-not-present transactions.

Note: The CSC check is fraud protection that verifies the card security code, also called the Card Verification Value (CVV2). The CSC appears only on the credit card itself, and not on acknowledgments or statements.

- None: To perform no CSC check, select this option.
- Full: To decline transactions when the CSC does not match or when the processor does not support CSC, select this option.
- Light: To decline transactions only when the CSC does not match, select this option.

7. In the **AVS Level** field, select whether to use the Address Verification System (AVS) with the configuration and at what level. For example, you may select to use AVS to process card-not-present transactions.

Note: The AVS is fraud protection that verifies customer billing addresses submitted through online payment transactions. With AVS, ***Blackbaud Merchant Services*** issues a transaction to authorize the payment. In response, ***Blackbaud Merchant Services*** receives information about the payment, including whether the street address and Zip code are correct. Depending on the AVS level selected for the account configuration, ***Blackbaud Merchant Services*** uses this information to determine whether to accept the payment. ***Blackbaud Merchant Services*** performs AVS only for transactions with addresses in the United States, United Kingdom, or Canada and does not decline transactions from other countries based on AVS.

- Full: To accept transactions only when both the street address and Zip code match, select this option.
- Medium: To accept transactions when either the street address or Zip code match, select this option. We recommend you select this option.
- Light: To deny transactions only when neither the street address nor the Zip code match, select this option. This level may accept transactions when either the street address or Zip code returns no response, regardless of whether the other criteria matches.
- None: To perform no address verification, select this option.

8. In the **Process mode** field, select the mode in which to use the configuration.
   - Live: To use the configuration to process live credit card transactions, select this option.
   - Test: To use the configuration to test ***Blackbaud Merchant Services*** and its connection to your Blackbaud program, select this option.
   - Demo: To use the configuration to demonstrate how ***Blackbaud Merchant Services*** processes credit card transactions, select this option.

9. To use Three-Domain Secure (3DS) authentication for card-not-present transactions processed through the configuration, select **Use 3DS processing**. For example, to use this configuration with a Blackbaud program that supports 3DS authentication, select this checkbox.

Note: The major credit card providers have developed 3DS as the authentication standard for online transactions. Examples of 3DS authentication include *Verified by Visa* and *MasterCard SecureCode*. 3DS authentication requires the cardholder to register the credit card through the card issuer's website and specify credentials used to verify online transactions.

10. Under **Supported credit cards**, select the checkboxes of the types of credit cards to process through the configuration.
11. Click **Save**. You return to the General Settings page.

Edit an account configuration

1. Under **Account Management**, click **General Settings**. The General Settings page appears.
2. In the Account configurations section, click the ellipsis next to the account configuration to edit and click **Edit**.
3. Edit the information as necessary.
4. Click **Save**. You return to the General Settings page.

Delete an account configuration

1. Your organization should maintain at least one configuration of your account with ***Blackbaud Merchant Services***.
2. Under **Account Management**, click **General Settings**. The General Settings page appears.
3. In the Account configurations grid, click the ellipsis next to the account configuration you want to delete and click **Delete**.
4. Click **Delete account configuration**. You return to the General Settings page.

Manage Multiple Accounts

If your organization creates multiple accounts with ***Blackbaud Merchant Services***, remember that each account has its own portal login credentials, and the portal displays only information about the account associated with the specific credentials used to log in. Your organization may provision multiple accounts with ***Blackbaud Merchant Services*** for various reasons.

- **Multiple credit card statement descriptors.** For example, your organization may want statement descriptors to refer to a geographic region, an affiliate, or a site, such as "Nonprofit Org SC" and "Nonprofit Org CA". Or, you may want to refer to specific fundraising campaigns or appeals in the descriptors, such as "Nonprofit Org RunWalk" or "Nonprofit Org Annual".
- **Separate reconciliation reports for multiple disbursement accounts.** Within the web portal, you can set up multiple account configurations and separate disbursement bank accounts. However, web portal reports provide information about all transactions processed through the overall ***Blackbaud Merchant Services*** account, not by configuration or disbursement account. To

generate separate reports for each disbursement account, you must create and configure a separate ***Blackbaud Merchant Services*** account for each disbursement account.

- **Multiple disbursement accounts for the same currency.** You cannot use the same currency with multiple disbursement accounts with a single ***Blackbaud Merchant Services*** account. To receive disbursements of the same currency type at multiple bank accounts, you must create and configure a separate ***Blackbaud Merchant Services*** account for each disbursement account.
- **Separate reconciliation reports or disbursement accounts for multiple events.** For example, your organization may want to analyze transaction reports or disburse funds into different accounts based on specific fundraising events. To do this, you must create and configure a separate ***Blackbaud Merchant Services*** account for each event.

Within each ***Blackbaud Merchant Services*** account you create, you can set up multiple configurations, such as based on credit card type or fraud protection levels, or to process card-present and card-not-present transactions or live and test transactions separately. Your organization must also set up a separate configuration for each type of currency you process through an account. For information about how to create multiple configurations of a single account, see Account Configurations on page 38.

Tip: For analysis of all transactions processed through multiple ***Blackbaud Merchant Services*** accounts, use the Blackbaud program through which you submit transactions.

Users

From the web portal, you can add and manage the users who can work with your ***Blackbaud Merchant Services*** account through the portal. When you add or edit a user, you can specify its login credentials and role, which determines which areas of the web portal the user can access. You can also manage the status of the user account, such as to unlock an account or disable an account for an extended period of time.

Note: The user's role determines the areas and features of the portal that the user can access. You can assign only one role to a user. For information about how to manage roles and grant feature permissions to roles, see Roles on page 45.

To view and manage your portal users, click **Users** under **Account Management**. On the Users page, you can view the display name, user name, status, and role of each user. You can also view details of when the user last logged in or changed the password.

From the Users page, you can add and manage users to the portal as necessary.

Add users to the portal

1. Under **Account Management**, click **Users**. The Users page appears.
2. Click **Add user**. The Add a user screen appears.
3. In the **Name** field, enter the display name to use to identify the user, such as the first and last name.
4. In the **User name** field, enter the name the user uses to log into the web portal.

5. In the **Password** and **Confirm** fields, enter the password the user uses to log into the web portal.
6. To require the user to change the password entered, such as for enhanced security, select **User must change password on next login**.
7. To grant the user rights to all areas of the portal, select **Grant administrative rights**.

   To grant the user rights to only specific areas of the portal, such as based on job responsibilities, select the applicable role to assign the user.

Note: The role determines the areas and features of the portal that the user can access. For information about how to create roles and grant feature permissions for roles, see Roles on page 45.

8. Click **Save**. You return to the Users page.

Edit a user

After you add a user to the portal, you can edit the detail information as necessary, such as to assign a different role. You can also manage the active status of a user as necessary.

Note: You cannot edit or delete the Administrator user account.

1. Under **Account Management**, click **Users**. The Users page appears.
2. In the grid, click the ellipsis next to the user you want to edit and click **Edit**.

   Warning: You cannot edit your own user account. If you attempt to edit your account, you return to the login screen.

3. Edit the details as necessary. To mark a user as inactive, deselect **Mark user active**.
4. Click **Save**. You return to the Users page.

Delete a user

When you delete a user, you completely remove the user from the database. Rather than delete a user, you can mark the user as inactive. To mark a user as inactive, edit the user and deselect **Mark user active**.

Note: You cannot edit or delete the Administrator user account.

1. Under **Account Management**, click **Users**. The Users page appears.
2. In the grid, click the ellipsis next to the user you want to and click **Delete user**.
3. Click **Delete user**. You return to the Users page.

Unlock a user account

If a user attempts to log into the web portal with an incorrect password five times, the portal automatically locks the user account to protect your ***Blackbaud Merchant Services*** account and information. From the portal, you can unlock users' accounts as necessary.

1. Under **Account Management**, click **Users**. The Users page appears.
2. In the grid, select the user to unlock and click **Unlock**.
3. Click **Unlock user**. You return the Users page.
4. Inform the user that the account is unlocked and to attempt to log in again.

Roles

From the web portal, you can add and manage the roles assigned to users who manage your account through the portal. Roles determine the areas of the portal each user can access. For example, for a user who manages only chargeback requests through the portal, you can create a Chargebacks role with rights to only the features available under **Chargebacks**. You can assign only one role to a user, so you can create and configure roles as necessary based on your users' needs. For example, if a user can access features from various parts of the portal, you can create a role with access to only those features and assign the role to the user.

To view and manage the roles available for your users, select **Roles** under **Account Management**. On the Roles page, you can view the name and description for each role. From the grid, you can add and manage roles as necessary.

Tip: To quickly add a role with similar permissions as another role, click the ellipsis next to the the existing role in the grid and click **Copy**. In the grid, the new role appears, which you can edit as necessary.

Add roles for users

1. Under **Account Management**, click **Roles**. The Roles page appears.
2. Click **Add role**. The Add a role screen appears.
3. Enter a unique name and description to help identify the role.
4. On the bottom of the screen, a list of all features in the portal appear. You can navigate the different categories of the portal to see different features. For each area, add the features that users in the role can access.
5. Click **Save**. You return to the Roles page.
6. To assign the role to a user, add or edit the user and select the role. For information about how to manage users, see Users on page 43.

Edit a role

After you add a role, you can edit its details as necessary, such as to grant or deny access to features.

1. Under **Account Management**, click **Roles**. The Roles page appears.
2. In the grid, click the ellipsis next to the role you want to edit and click **Edit**.
3. Edit the details or feature permissions as necessary.
4. Click **Save**. You return to the Roles page.

Delete a role

After you add a role, you can delete it, such as if no users require it. You cannot delete a role assigned to a user. To remove a role from a user, first edit the user to assign a different role. For information about how to manage users, see Users on page 43.

1. Under **Account Management**, click **Roles**. The Roles page appears.
2. In the grid, click the ellipsis next to the role you want to delete and click **Delete**.
3. Click **Delete role**. You return to the Roles page.

Mobile Devices

With the ***Blackbaud MobilePay*** mobile application, you can accept credit card transactions through a mobile phone or tablet and process the transactions through your ***Blackbaud Merchant Services*** account. Click **Mobile devices** under **Account Management** to add and manage the mobile devices that access your account. On the Mobile Devices page, you can view the name, status, and security code of each device.

When users first download the mobile application, they enter their login and add a unique name for their device and then have 30 minutes to process transactions until their device is approved. Then, you can approve a device or decline access as necessary. You can also suspend access for any device after it has been approved, such as when the device is lost, stolen, or otherwise not in use.

Note: To maintain an audit trail, you cannot delete mobile devices once they have been added.

Manage mobile devices

1. Under **Account Management**, select **Mobile devices**. The Mobile Devices page appears.
2. To approve a pending device, select the ellipsis next to the device you want to edit and select **Approve**.
3. To edit the status for a device, select **Edit**. You can suspend, decline, or reactivate approved devices.