

Ecommerce Guide # 1:

Navigating our BackOffice



Best Practices



**Establishing
Transaction Rules**

Navigating our Back Office

Login to our Back Office by clicking on <http://login.merrco.ca> using credentials established upon activation

Secure Merchant Login

User name

Password

[Forgot your password?](#)

support@merrco.ca
1-888-709-8753

Once in our Back Office you will see the following menu panel:

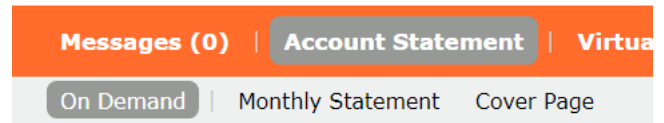


Messages (0) | Account Statement | Virtual Terminal | Batch Upload | Reports | Customer Profiles | Settings |

Message Centre: Summarizes key system notices and alerts for review and requiring attention

Account Statement: The Account Statement tool provides you with immediate, current information on your account with Paysafe. Your account is actually subdivided into three sub-accounts, which you can view at any time. The Account Statement tab also has the Monthly Statement sub-menu. The Monthly Statement provides a monthly report (from the first to the last day of previous months) on activity in your merchant account. Each report includes a summary of total sales, total credits, discount fees, transaction fees, and other monthly fees – all grouped by card brand.

- a. On Demand: Provides a view of transactions in the date range selected
- b. Monthly Statement: Downloads your monthly statements



Virtual Terminal: Process credit/debit card transactions manually directly through the back-office portal

Batch Upload: Process transactions by uploading CSV or XML files containing your transaction requests. You can upload the following files: Credit card transactions; Direct Debit transactions and Recurring billing records

Reports: Generate activity reports using account numbers, card numbers, etc. to view transaction details.

- 1) Generate batch reports to view transaction and batch details;
- 2) Generate chargeback reports to view a summary and details of disputed transactions;
- 3) Drill down on an activity report to process transactions like Settlements and Credits (see next diagram); and

Purchase Fully Settled

Txn ID:

Account: 100

(S: CAD | P: CAD)

Consumer Information		Billing Details	
Name	--	Address	--
Email address	--	Address (cont'd)	--
Phone number	--	City	--
IP Address	--	Province	--
		Country	CA

Authorization Information		
Merchant Trans. ID	Frequency	One Time
Date	Auth Code	
Auth. Conf. No.	Auth Mode	Purchase
Amount	Auth Type	Final
Remaining to Settle	AVS Response	MATCH _ZIP_ONLY ?
Card Details	CVD Response	MATCH ?
Txn ID	Pay Proc Response	ZIP MATCH
Apple Pay	ECI Code	Failed authentication or not a 3D Secure transaction - no liability shift
Google Pay	IP Address	35.183.

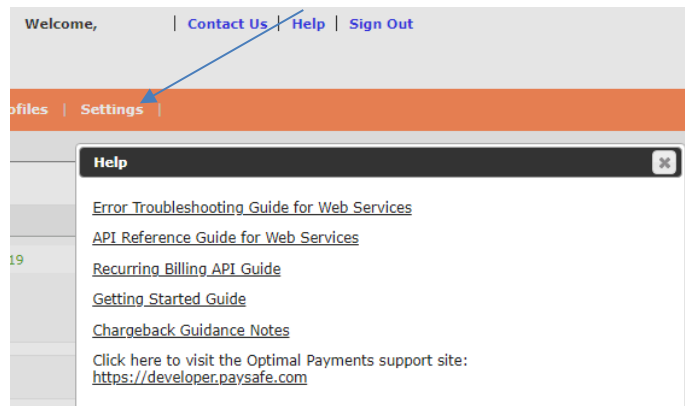
Date	Txn ID	Merchant Trans. ID	Status	Remaining	Amount	Batch ID	Batch Date	ARN	Acquirer Txn ID
2020-07-			Completed	5.65	5.65		2020-07-01		

4) Schedule pre-configured reports to receive via email or SFTP. (Refer to our Guide on Setting up reporting in our BackOffice)

Customer Profile: The Customer Profiles tool allows you to create customer profiles, which in turn can contain recurring billing records that will ensure regular, trouble-free payments from your customers for goods or services you provide on a regular basis. Once you set up a customer profile with a recurring billing record, BackOffice does the rest, processing the recurring transactions for the amount, at the frequency, and over the time period that you specify. The Customer Profiles tool also allows you to search for customer profiles to view their status and/or modify them at any time. In addition, you can process single, unscheduled transactions using the credit card and customer information contained in a customer profile

Settings: Create and modify back-office users • Create and modify email templates for communication with your customers. • Change your password. • Set your default landing page in the back office. • Set the currency format for Virtual Terminal and Activity Report functions (i.e., amounts with or without decimals).

Getting Help:





Best Practices for Ecommerce transactions

CHECK: PAYMENT RESPONSES IN OUR BACK OFFICE

- AVS response on the Merrco Back Office is a positive match
- CVD response on the Merrco Back Office is a positive match

COMPARE: CHECKOUT CART INFORMATION WITH INFORMATION IN OUR BACK OFFICE

- Billing address vs. shipping address (please pay attention to PO Boxes given as shipping address)
- Card BIN country with IP country
- IP country with Billing and Shipping addresses

FLAG: FOR FURTHER REVIEW

- Unusually high-ticket amounts
- Multiple transactions with same card/address/email address/phone number/customer name/IP within a short period of time
- Multiple transactions where one detail overlaps (such as name, email or IP address) but different cards/address/email address/phone number are used.
- Transactions using an email address, billing address, IP address or phone number associated with another transaction declined due to reason code 3016 (card reported as lost/stolen)

REQUEST: FOR FURTHER ASSURANCE

- A copy of identification verifying the customer's identity
- A copy of the front of the credit card used (with only the first six and last four digits showing). Please note that it is not PCI compliant to retain a copy of full card number and/or the back of the card.
- Signature upon delivery or pick-up
- Tracking information for delivery
- Written authorization from the cardholder (this is not necessarily the same as the customer)

IMPLEMENT REPORTING (Refer to our Guide)

- Chargeback Reporting
- Velocity Reporting

REMEMBER:

It is always best to cancel orders and refund transactions as quickly as possible if you are not comfortable with the purchase for any reason. For click and Collect customers you can offer to have them pay in-store via POS -Chip and Pin

Once a transaction is charged back, the funds revert to the cardholder. At that point, the only possible actions to potentially recoup the funds are to request the cardholder cancel the chargeback if it was in error or resolved and have them provide confirmation once the chargeback is cancelled.

If the Cardholder is not willing to do so then you should dispute the chargeback. (refer to our Chargeback & Dispute guide)



Risk Rules: Set your level of transaction control

The following rules are available to apply to your merchant account which you may find beneficial depending on your business model. If you would like to implement any of the below, please contact us at risk@merrco.ca and advise as to the rule and the merchant account to which it should apply.

Card-based Risk Rules

1. **Transaction Cap:** this rule will decline all transactions over a pre-determined amount set by you.
2. **Card-Specific Transaction Cap:** this rule will limit the total amount *successfully processed* through a particular card for a given number of days and decline further transactions from that card for that defined time period as set by you.
3. **Velocity Rule:** this rule will allow you to set the number of transaction *attempts* or successful transactions allowed per card and decline further transactions from that card for a defined period of time as set by you.

Email Address-based Risk Rules: *please note that the following rules may not be available to you depending on your integration.*

1. **Velocity Rule:** this rule will allow you to set the number of transaction attempts allowed per email address and decline further transactions from that email address for a defined period of time as set by you.
2. **BIN Country Rule:** this rule can decline all transactions from a particular email address for a set number of days as defined by you if the BIN country presented in a transaction does not match the country of the billing address.
3. **Multiple Cards:** this rule can decline all transactions from a particular email address for a set number of days as defined by you once a given number of different cards are used in transactions processed through your merchant account and associated with that email address.
4. **Lost/Stolen Cards:** this rule can decline all transactions from an email address once it is associated with the use of a card reported as lost/stolen for a given number of days as defined by you.
5. **Domain:** this rule can decline all transactions from a particular email address domain that you deem likely to be used in perpetuating fraud.

