MERCURY®

Welcome

Mercury Welcome Guide

Enter your merchant number and bank ID number information here (numbers provided to you in your Mercury® Welcome Package):

Merchant number

Your bank ID number

Voice authorization numbers
Visa®/MasterCard®/Discover®: 800.944.1111
American Express®: 800.528.2121

Code 10 authorization number
800.944.1111

Code 10: A universal code that merchants can use to alert the authorization center that a suspicious transaction is occurring without alerting the cardholder.

See page 26 & 27 for more information.

Mercury Confidential and Proprietary - For Recipient's Internal Use Only

Troubleshooting

Our MercuryLive™ customer care and technical support team is available around the clock.

Call: 800.846.4472
Email: ics@mercurypay.com
Chat: Logon to the MercuryView® portal and click Contact Us. Select Live Chat or Web Wizard.

Please contact MercuryLive with the following issues:

MercuryView
For help logging in or using the MercuryView portal, please contact our support team.

Unable to process
Confirm your internet connection through your internet service provider and verify your network activity. If these steps do not result in a resolution, please contact our support team.

Unable to process single transaction
You can confirm the transaction via our online portal at www.mercurypay.com. If you need help with the website please contact our support team. You can also call to get a voice authorization guaranteeing funds will be pre-authorized. Please refer to voice authorization information on page 11.

Batch totals do not match
You can confirm your totals via our online portal at www.mercurypay.com. If you need help with the website, please contact our support team.

Computer/hardware problems
Our support team is available to assist with basic POS troubleshooting however you may need to contact your POS reseller for certain computer/hardware issues.

Contents

MercuryView

Logging on to Your Mercury Home Page

To log on to your Mercury home page:

- Go to www.mercurypay.com
- Enter your user name and password, click Sign In
- For help logging in or using the MercuryView portal, contact Mercury at 800.846.4472

Reporting

Over 30 reports can be accessed from MercuryView. You can use saved reports or create your own using custom criteria.

Saved Reports – A quick and easy way to reconcile your recent transactions.

Custom Criteria – Customize a report based on your current needs. For instance, you can create a report to help you troubleshoot or reconcile your batch. For assistance in creating custom reports, call MercuryLive customer service at 800.846.4472.

In addition to transaction reports, credit card processing statements are also available online. Your batch detail and deposit reports are updated daily so you can keep track of your anticipated deposit volume, and daily discount totals from the last closed batch. The statements display batch details, chargebacks and retrievals, deposit totals, returns and more. You will be able to view processing statements from the previous 18 months. Download them to your own file and keep them year round, or print them for your records.

The online statements contain proprietary financial information that you may not want to share with other MercuryView portal users in your business. Anyone who has access to your portal username and password will also have access to your

daily deposit, settlement information and processing statement. You can reset your password at any time to ensure privacy and provide other employees with their own login information.

By managing your portal Account Settings, you can control which portal users have access to your reports. You will be able to allow other users, including your POS dealer, to view the real-time transaction reports without viewing your financial statements.

Additional Tools

Additional resources are available in MercuryView including:

- Frequently asked questions
- Glossary
- Account setting and contact information
- Online technical support options
- Bulk processing forms
- Web reporting guide

Transactions

Transaction Types

There are seven different types of transactions:

Pre-authorization Transaction – a transaction verifying whether the card is valid, active, and has funds available. A pre-authorization sets funds aside, and the merchant receives an approval code freezing those funds. A pre-authorization typically sets these funds aside for 7-10 business days, after which the funds are unfrozen. The specific time for which the funds are set aside varies depending on the card-issuing bank.

Pre-authorization Capture Transaction – a transaction that finalizes the pre-authorization transaction and charges the cardholder when the merchant completes the sale. Pre-authorization and Pre-authorization Capture transactions are most commonly used in restaurant environments.

Sale – a transaction that combines two operations (authorization and capture) into one transaction. Used most in retail transactions.

Return – a transaction that puts money back into a customer's card account after the batch is closed.

Adjust – a transaction that changes the amount of a transaction in the current batch.

Void – a transaction that voids a captured transaction. NOTE: A void can only be used on transactions in the current batch. Funds may still pend on on the customer's account even if a void is processed.

Voice Authorization – see next page.

Voice Authorization

A voice authorization is an authorization that is given over the phone from the card-issuing company (Visa®/MasterCard®, Discover®, etc.). To obtain a voice authorization, the merchant must call the appropriate voice authorization phone number and receive a six-digit authorization code. (See below.) The merchant must then perform a voice authorization transaction by keying the authorization code into the POS to capture the transaction and receive funding. For example, if a merchant swipes a card and receives a "Call ND" message, a voice authorization must be obtained by calling the authorization number for Visa/MasterCard/Discover.

Reasons to Get a Voice Authorization

The most common reasons requiring a voice authorization are:

- Card doesn't swipe
- Unusually large transaction
- Internet connection goes down
- Suspected fraud
- Power outage

Voice Authorization Support*

Common error messages:

MUST BAL NOW
You must settle your batch before you can run another transaction.

Call Center
Call Visa/MasterCard/Discover

Error Response Code
Call Visa/MasterCard/Discover

Call ND
Call Visa/MasterCard/Discover

Call AE
Call American Express

Voice Authorization Numbers - US
Visa/MasterCard/Discover: 800.944.1111
American Express: 800.528.2121
Diner's: 800.525.9040

Voice Authorization Numbers - Canada
Visa/MasterCard: 800.268.8241
Discover: 800.268.6362
American Express: 800.268.9824

*When you call for a voice authorization, those funds are pre-authorized off the card.

Settlement

The process of transferring funds from the cardholder's financial institution to your bank is called a settlement. There are two ways in which batches are closed, depending on how your POS system is set up: time-initiated, or merchant-initiated settlement. If you are not sure what type of system you are using, contact your POS dealer or Mercury at 800.846.4472.

Time-Initiated Settlement (auto-close)– closes the batch automatically.

Merchant-Initiated Settlement– requires the merchant to manually settle the batch through the POS system.

Chargebacks

Your Right to a Rebuttal

A chargeback is a transaction that is being disputed by the cardholder or his/her issuing institution. A chargeback occurs when a cardholder disputes a charge or when proper bankcard acceptance and authorization procedures were not followed. If you receive a chargeback, your deposit account is debited for the indicated amount. **Please refer to page 15 for frequently asked questions regarding chargebacks.**

These examples represent 90 percent of all chargebacks:

- Cardholder authorization was not obtained
- Requested/Required authorization was not obtained
- Recurring transactions have been cancelled, i.e. a health club membership
- Duplicate processing occurred
- Services were not rendered
- Cardholder did not receive merchandise
- A credit was not processed
- An expired card was used
- Requested transaction data was not received
- Account number used is not on file

What to do with a...

Retrieval request. You should immediately pull your originating documentation for the transaction in question and fax it and the retrieval request to Global Payments at 443.394.1915.

Chargeback. You should read the reason for debiting your account on the form. If it is incorrect, immediately fax supporting documentation and the notification of chargeback to Global at 443.394.1915. If the issuing bank accepts your documentation, the chargeback will be reversed and the amount of the disputed transaction will be credited to your account. This credit is conditional. If the cardholder disputes the reversal, a second chargeback may be initiated. In addition, if your documentation does not support your case, the chargeback debit to your account will remain. Retrieval requests and notification of chargebacks should be responded to as soon as possible. **The fastest way to respond is by faxing the requested documentation to 443.394.1915. If you do not have access to a fax machine, mail your documents to: Global Payments, Department CED, 10705 Red Run Boulevard, Owings Mills, MD 21117.**

Do's and Don'ts

You can significantly reduce the chance of receiving a chargeback notification by taking the following precautions:

Do:

- Understand that you assume all responsibility for the identity of the cardholder for all fax, internet, mail order and telephone order sales.
- Prepare and submit a written rebuttal within the time specified on the chargeback notification.
- Accept cards where the cardholder account number is valid.
- Authorize all sales.
- Verify arithmetic on sales drafts.
- Charge the cardholder for the correct amount.
- Credit the cardholder for the returned merchandise.
- Credit the cardholder for the canceled order.
- Verify that the signature on the sales draft matches the signature on the card.
- Verify the authorization code.
- Obtain a manual card imprint if unable to capture from magnetic stripe.

Don't:

- Accept sales that are declined, and if a sale is declined, do not attempt authorization a second time on a declined sale. The cardholder bank may collect an additional fee if you fail to follow card acceptance and authorization procedures.
- Charge a cardholder before shipping the merchandise.
- Accept sales that are not authorized for the exact amount.
- Accept an expired card.
- Accept a card before the effective date on a dual dated card.
- Process a credit as a sale.
- Deposit the sales draft more than once.
- Deposit an incomplete sales draft.
- Accept a sales draft without the cardholder's signature.
- Participate in a suspicious transaction.
- Obtain an authorization by using multiple transaction/split sales drafts.
- Accept a card where the account number obtained off the magnetic stripe does not match the account number on the draft.

Chargeback FAQs

What is a chargeback?

When a credit card transaction is disputed (either at the request of the cardholder or by a card issuer), the dispute is handled through a chargeback. A chargeback will cause the amount of the original sale and a chargeback fee to be deducted from the checking account you provided on your application. The credit card associations only allow a limited amount of time to respond to a chargeback. It is critical any response be provided by the date requested on the chargeback notification.

What is a retrieval request?

A retrieval request occurs when your customer requests more information about a transaction that appears on his or her credit card statement. A response must be submitted by the date requested on the retrieval request notification to avoid a non-reversible chargeback.

Are funds deducted from my bank account as a result of a retrieval request?

No, a retrieval request is just a request for information. The amount of a retrieval request is not deducted from your bank account.

When will I be notified of a chargeback and when are funds removed from my checking account?

The processor will usually mail a notification of chargeback when the debit is transmitted

to your bank. Most often, you will receive notification at the same time your checking account is debited.

Why did I receive a notification of chargeback without a prior retrieval request?
Not all chargeback reasons require the issuer (cardholder's bank) to generate a retrieval request before initiating a chargeback.

I won my chargeback, why did I still receive a charge?
Whether a chargeback is won or lost, the issuing bank still charges a handling fee, typically $15.50. This fee is non-refundable.

How much do chargebacks cost me?
When a chargeback is initiated, the amount of the transaction in question is deducted from your account, along with a non-refundable chargeback processing fee of $15.50. It costs you nothing to reverse a chargeback, when possible, and upon reversal, the transaction amount in question will be credited to your account.

Is the risk of chargeback greater if I manually enter the credit card number?
Yes. If you complete a transaction where a card is present but you do not get an imprint (manual or electronic) of the card, you may lose money through a chargeback when the cardholder disputes the transaction. This does not apply to mail order/telephone order merchants.

Who is going to pay for my bounced check fees because this chargeback was taken from my account?
Per the terms and conditions of the merchant contract, it is your responsibility to have enough funds in your account, any bounced check fee remains your responsibility.

I issued a credit and I still received a chargeback. Why?
In this case, the issuer did not see the credit issued by you. If the credit was issued after the chargeback was initiated, provide the appropriate documentation of the credit.

How long should I keep my receipts?
Receipts should be kept in a safe place for a minimum of two years.

How do I prevent chargebacks?
If a transaction is a mail order or telephone order, use a form of shipping that provides proof of delivery. For higher ticket items, require a signature for delivery. If the card is not present, attempt to get the CVV2 data from the cardholder. Also, pay attention to the Address Verification System (AVS) response received. Do not accept numbers and information that do not come back as a match. Use common sense in shipping to an address other than the buyer's billing address. International transactions represent an even higher risk. If a credit needs to be issued, ensure that the credit is issued to the same credit card used to make the purchase. Finally, know who you are dealing with by verifying the signature on the back of the card to the signature provided. If the signature is not present on the card, request card holder identification. If in doubt, do not hesitate to contact us or call the applicable voice authorization number with a "Code 10" request.

If I have questions, who do I call?
Mercury will be happy to help you with any question you may have. Please contact us at 800.846.4472.

I was told that an authorization guaranteed payment.
An authorization will only verify that an account is open and that there are funds available. However, if a card has been

lost or stolen and the loss has not yet been reported, any charges made by the criminal can later be charged back by the cardholder.

I sent in the required documentation, but still received a chargeback.
If the chargeback was not responded to by the required date, or if a lost or stolen card was used for the disputed transaction the chargeback will stand. It is your responsibility to verify the person involved with the transaction is the actual cardholder.

Funding and Statements

Batch Closures

There are two types of batch closures: time-initiated and merchant-initiated. Time-initiated will automatically close at either 10 p.m. EST or 4 a.m. EST each day for prompt funding. Merchant-initiated batch closures should occur no later than 5 a.m. EST for prompt funding. Transactions occurring after the cut-off time will be carried over to the next batch.

Deposits

A batch closure creates a corresponding deposit. Without a batch closure, there can be no deposit. Bank records will reflect a deposit in approximately two business days on a typical week. If the deposit is made on a weekend or a holiday, it may take a day or two longer to reflect the deposit.

Mercury makes deposits to your bank account for Visa, MasterCard, and Discover. Debit, EBT, and food stamps will be separately deposited by Mercury. For some merchants, Discover makes its own deposits to your bank account.

American Express makes its own deposits to your bank account. Such deposits are not funded with your Visa, MasterCard and Discover transactions. **American Express' contact number is: 800.528.5200**

Statements

Statements are sent on the fifth day of every month and are also available online within a few days after the statement has been generated. Processing fees are taken out of your account on the first of each month. If you believe your statement is incorrect or you have any questions regarding your statement or transactions, **please contact Mercury at 800.846.4472.**

Best Practices

Following best practices when accepting credit and debit cards will assist you in treating all customers fairly, and in honoring cards without discrimination. It will also assist in being vigilant about security.

You may ask for personal information when...

- Store policy is to request it for all payment methods including checks and cash. You cannot make providing information a condition of the sale, unless local laws allow.
- You need this information to deliver an order.
- The authorization operator specifically requests you obtain it.
- The card is not signed and you must have the cardholder sign it and check the signature against another piece of identification.

You may not...

- Ask for a customer's debit PIN number.
- Assist a customer in a manner where the PIN number will become exposed. (Security cameras should not be pointed so they photograph customers entering PIN numbers. The PIN number belongs to the customer and needs to be protected.)

Never honor a bankcard when...

- The customer does not have the actual bankcard.
- The card appears to have been tampered with or altered.
- Authorization is declined, or you're told to "pick up" the card.
- The signatures do not match.

PCI Data Security Standards – Myths & Merchant Responsibilities

PCI myths

- If a merchant is running a PA-DSS compliant payment application, nothing more is needed.
  - ✔ Running a PA-DSS compliant application is only one of 12 requirements of PCI-DSS.
- My dealer told me I'm PCI compliant.
  - ✔ You may not be compliant unless you're getting quarterly network scans and have completed your annual Self-Assessment Questionnaire. Your dealer was most likely referring to the compliance of the POS application you use.
- PCI compliance is just too complicated.
  - ✔ Not necessarily. The requirements for PCI-DSS are best practices that all businesses (regardless of size) should follow.

- A breach won't happen to me.
  - For small merchants it is not a matter of if but when they will be breached. Data thieves are targeting small merchants daily.

Merchant PCI-DSS responsibilities

1. Install and maintain firewalls – software firewalls and router/firewall hardware are not sufficient to properly protect your POS system. See #10 below.

2. Change all vendor supplied passwords – make sure that all administrative, remote access and default passwords are changed. Use complex passwords with both letters and numbers that are at least seven characters in length.

3. Protect stored cardholder data – if your POS system stores any card data, it must be encrypted and secured. If you retain paper receipts with full card numbers for record keeping purposes, they must be locked up and shredded when no longer needed.

4. Encrypt transmission of cardholder data across open, public networks – any transmission of card data must be made over SSL encrypted communication channels.

5. Use and regularly update anti-virus software – make sure that your anti-virus definitions are up to date and that you annually renew your subscription.

6. Develop and maintain secure systems and applications – all merchants must use a PA-DSS compliant point of sale application.

7. Restrict access to cardholder data to only those people who need access to it.

8. Assign a unique ID to each person with computer access – everyone who has access to the POS system must have a unique username.

9. Restrict physical access to the cardholder data – keep your POS computer in a locked cabinet or office.

10. Track and monitor all access to network resources and cardholder data – install a business level hardware firewall that is capable of inbound/outbound filtering – only allowing traffic from known sources (such as Mercury) to access your network.

11. Regularly test security systems and processes – have external networks scanned for vulnerabilities once a quarter by an Approved Scanning Vendor, and complete an annual Self-Assessment Questionnaire.

12. Maintain a policy that addresses information security for all personnel.

Practical steps to reduce your risk

DISCONNECT security cameras, wireless access points and other computers or devices from the POS network segment.

STOP all internet browsing from systems connected to the POS network segment.

CONDUCT a quarterly PCI vulnerability scan.

SCHEDULE regular anti-virus scans and definition updates.

APPLY all operating system patches and POS updates as soon as they are released.

ENABLE remote access only when needed; disable when done.

SEGMENT all other computers and devices from your POS network including wireless, back office computers and laptops.

EDUCATE your employees annually about security best practices.

ENROLL in Merchant SecureAssist®, Mercury's PCI compliance solution.

Fraud

Don't be bullied

If a customer attempts to intimidate a cashier by causing a fuss at the register, it may be to rush the purchase, causing an improper checkout. The customer may tell you that the card won't read and not to bother running it through – that you'll have to key it in manually. In such instances, customers have also been known to complain about the service or length of the line. They may even demand to see a manager – anything to keep the cashier's attention off the authorization of the credit card.

Never call a telephone number given by the cardholder for authorization. Don't be intimidated by these bullies; always take your time and make sure the correct procedure is followed when authorizing the card.

Borrowed cards

Beware of people presenting letters of authorization for use of a credit card. Under no circumstances are these letters an acceptable form of verification or authorization. Friends, coworkers, children and spouses are not permitted to borrow each other's cards. The only person who should be presenting the card to you is the person whose name is on the front of the card and signature on the back of the card. Most often, the rightful owner gets the statement and a chargeback inevitably occurs.

The manual key-in

Often fraud occurs when the thief damages the card on purpose so that you are forced to manually enter the number in the electronic point-of-sale terminal. Fraudulent cards are often damaged in order to bypass the antifraud features that are placed on them – the magnetic stripe cannot be swiped and transmitted to the verification center for authorization in the case of a manual key-in.

If you have an electronic point-of-sale terminal, swipe every card that is handed to you, no matter how damaged or worn. Be wary of customers who let you know right away that their card won't read. If the card doesn't work and you end up keying in the number, make sure you take an imprint of the card. If the card is severely damaged, simply ask for another form of payment.

Fraudulent returns

It is estimated that, on average almost six percent of holiday returns are fraudulent.[1] Make sure your employees and customers are well informed of your return policies and monitor return activity using MercuryView.

Counterfeit cards

Stolen and counterfeit cards are a costly problem for merchants and credit card issuers alike. Because of the technology available to them, counterfeiters are able to reproduce false cards that are high quality, even without the benefit of the original. All they really need is personal information and technology to produce credit cards, debit cards, and smart cards.

The purpose of Code 10

Any time you have doubts about something – a fraudulent card, a signature or even a customer's behavior–call in a Code 10. A Code 10 allows you to call for an authorization without the customer becoming suspicious.

After dialing the authorization center, inform the operator that you have a Code 10. The operator will put you through to the correct person, who will ask you a series of "yes" or "no" questions. Hold on to the card if possible while making the call. If the operator decides something is amiss, he or she will deny authorization. The operator may even request to speak to the cardholder to ask account information questions that only the true owner of the card would know.

A Code 10 can be used any time you feel a transaction may not be legitimate, even if you have already received approval on a transaction or if the customer has already left the premises.

When to call in a Code 10:

- If the embossing on the card is illegible.
- If the last few numbers are not embossed on the hologram, or if these numbers do not match the account number on the sales draft or at the terminal.
- If there is no Bank Identification Number (BIN) above or below the first four digits.
- If the name on the card does not match the signature or there is a misspelling.
- If the hologram is not clear or the picture in the hologram does not move.
- If the card does not have an expiration date.
- If the card does not start with the correct numeric digit (all Visa cards should start with a 4, all MasterCards with a 5, all Discover cards with a 6).
- Be aware of cards that don't swipe; check these cards for other security features.
- If a card does swipe, make sure the card number and the number that appears on the terminal match.

Risky business

Card processors like Mercury monitor merchant transactions for signs of fraud or abuse. This protects merchants and cardholders. Certain kinds of merchant behavior are not allowed and could result in the termination of your account.

Don't ever use your own card to give yourself a cash advance. If you need to perform a transaction that is out of character for your business, give us a call first. For example, if you are a restaurant that typically does $30 swiped transactions, call us before you run a $5,000 sale for a catered wedding.

Tips on fraud prevention

1. If a photograph of the cardholder is present on the card, you should compare the photograph on the card with the person presenting the card.

2. Check cards for the hologram. A hologram is a three dimensional symbol in either gold or silver foil that is designed to help deter counterfeiting. The image should reflect light and appear to move when you tilt the card. NOTE: The Visa hologram is an image of a dove; the MasterCard hologram is an image of a world map; the Discover hologram has four distinct images.

3. Check cards (including the signature panel) to see if they have been altered.

4. Check the valid date (some cards are not valid until the date shown) and the expiration date on the face of the card. If the card is not yet valid or expired, you should not accept the card and should instead ask for another form of payment. NOTE: Cards are valid through the last date of the month, unless an exact date is displayed.

5. For each card type, be aware of the first four digits and the total number of characters. NOTE: A Visa-branded card number begins with a "4" and has 13 or 16 digits; a MasterCard-branded card number begins with a "5" and has 16 digits; a Discover card number begins with a "6" and has 16 digits.

Check the first four digits of a card. For Visa and MasterCard, the first four digits of the embossed card number must match the four digits printed above or below that number on the front of the card.

6. The account number on the front of the card should match the number printed on the back of the card in the signature panel. For Visa, American Express and Discover, compare the entire account number imprinted in the signature panel with the embossed account number on the face of the card.

For MasterCard, compare the four-digit truncated account number imprinted in the signature panel with the last four digits of the embossed account number on the face of the card.

For MasterCard, contact your acquirer for instructions if:

- You believe there is a discrepancy in the signature.
- The last four digits of the embossed account number do not match the four digit truncated account number on the signature panel or displayed on the terminal.
- The photographic identification is uncertain.

If any MasterCard does not have a MasterCard hologram on the lower right corner of the card face, confiscate the card and contact your acquirer's Code 10 operator for instructions on card pick-up and mailing.

7. Attempt to swipe every card through a POS terminal. If the terminal cannot read the card, you should take a manual imprint of the card. When using a manual imprinter, you should check the draft for a clear impression of the card to ensure that you have captured the embossed card account number.

Complete the draft with the date, description of merchandise/service, sales tax, total dollar amount and authorization number, and get a signature.

8. Never allow customers to tell you how to "get the transaction to go through" (for example, by doing a ticket only transaction without getting an authorization). This will likely result in a chargeback, and these customers will have "stolen" or obtained items for free.

9. Obtain customers' signatures. The signature on the draft must match the signature on the back of the card.

10. If a customer's card is unsigned, request another form of identification with a photo and signature. Request that the customers sign their cards and then compare the two signatures.

If a customer refuses to sign, inform them that you are unable to accept an unsigned card for payment and then request another form of payment. The card association rules dictate that card acceptors must not complete the transactions if cardholders refuse to sign the card.

Visa, MasterCard, and Discover's websites provide materials designed for merchant use and offer tips on what merchants can do to prevent fraud.

11. Use caution when taking an international order. Fraudulent transactions that originate overseas are on the rise. Remember that international transactions are high-risk transactions. Know your customer. Properly identify the person with whom you are dealing. Take a second look at what is being ordered and where it is being shipped. Did your customer offer you multiple cards as payment? Is the customer asking for immediate shipment? If so, you may have just detected a fraudulent transaction and saved yourself from taking a loss. There is a tremendous amount of fraud with international transactions, and it is virtually impossible to win the chargeback case. Banks outside the U.S. may not support additional security features like AVS, CVV2, and Verified by Visa®. If in doubt, do not hesitate to contact Mercury and we will be happy to assist you.

12. Utilize security functions such as entering the "last four digits" of the card on swiped-card transactions and Address Verification and CVV2 code to discourage use of counterfeit cards. Verified by Visa® and MasterCard SecureCode™ are payment initiatives designed to reduce the risk of unauthorized use of cardholder account by authenticating the cardholder attempting to make a purchase online. Authentication makes internet shopping better and safer for both buyers and sellers by reducing the merchant's exposure to fraud and frivolous disputes, and protecting the cardholder from fraudulent use of his/her card. Implementing Verified by Visa shifts liability away from the merchant and onto the card issuer.

13. If you are going to run an unusually large transaction, or if you need to manually key numerous transactions when you usually swipe your credit cards, call ahead to let Mercury know what you are doing. Otherwise, your account may be flagged for unusual and suspicious activity, which may cause your funds to be held.

[1]National Retail Federation, Retailers Estimate Holiday Return Fraud Will Cost Them $3.4 Billion, According to NRF Survey, https://nrf.com/media/press-releases/retailers-estimate-holiday-return-fraud-will-cost-them-34-billion-according-nrf, (December 2013).

800.846.4472
150 Mercury Village Drive | Durango, CO 81301