Announcing: Risk Management Top Ten List

At some point of your merchant's processing life, they might end up working with our Risk Management team over a transaction(s) they processed. A lot of the times, these issues could have been avoided by the merchant, or by the Sales Partner. Below are some helpful tips that may assist you in working through some of our common risk related issues:

Risk Management Top Ten List

1. Average Ticket / High Ticket provided on merchant application
2. Monthly Volume amounts
3. Deposit delays due to keyed transactions
4. Presentation of sales drafts, invoices, and delivery notifications
5. Off-shore fraud scams targeting merchants
6. Improper issuance of consumer sale credit
7. Transactions using business owner's own credit card
8. Problems associated with "custom orders"
9. Previous poor merchant activity resulting in a MATCH listing
10. Failure to comply with 3rd party Site Survey

We hope that improving your knowledge of these ten common situations that your merchants can reduce their potential for being contacted unnecessarily by our Risk Management team. In doing their due diligence, they might come across a merchant which has the appearance of requiring a review, but ultimately never needed to be in that situation.

Please review the detailed information below as highlighted above.

1. Average Ticket/High Ticket- Please confirm, with the merchant, that these parameters are as accurate as possible, as the given amounts are what Risk Management is expecting to see being processed. If such information is incorrect, Risk Management may not be able to avoid having to delay the funding to the account, if a larger than presumed sale is processed; this will lead to certain frustration not only for the merchant but for the Sales Partner as well.

2. Monthly Volume- Like the aforementioned ticket amounts, it's important that Risk has a good idea of how much merchants will be processing on a monthly basis. Because an ISO is liable for 180 days on all merchant's credit card sales, a processor, for all intents and purposes, is extending a line of credit to a merchant for a period of six months on each transaction. If a merchant is processing above the Monthly Volume for which the account was underwritten, it is likely that the merchant will be asked to provide financial records that reinforce the higher volume. Understandably, most merchants do not like to provide such information once an account has been approved, so to avoid such an issue, it is imperative that Risk has a full understanding of a merchant's monthly volume.

3. One of the most common reasons a merchant's deposits are delayed is due to credit cards being manually entered through a retail account. By processing in such a manner, a merchant is waving certain rights that he would normally have through the Visa/MasterCard dispute process. Without this insurance, Risk must take extra precautions by reserving the funds of these sales, until documentation can be reviewed, and verified, with an issuing bank. If a merchant indicates that he will be keying a large portion of his transactions, he should 1) be set up on a MOTO platform and/or 2) be advised that valid imprints, complete with the merchant's nameplate, must be obtained. The above-mentioned nameplate is included in all merchant welcome packets. If a merchant does not denote how he will be processing cards, please clarify this point with him.

4. From time to time, Risk Management may request documentation from a merchant. Such data includes, but is not limited to, invoices, contracts, proof of delivery/job completion, and sales receipts. Please advise merchants that such requests may be made, so they are not caught off guard if they are contacted for these purposes. Please also reassure them that this information will only be used for verification needs. Having this information ahead of time may help reduce any reservations a merchant may have in providing supporting documentation. It may also be wise to inform the merchant that he is required, per his agreement with TMS, to keep a card-holders name, billing information, and a description of rendered services on file, in the event it is requested for verification purposes.

5. Increasingly over the last decade, every-day merchants are being targeted by scams originating from overseas, especially from Southeast Asia and Africa. The scam is to contact the merchant, place an order (usually a very large order, enticing the merchant to consider the potential profits instead of sound judgment) and then pay for that order with a stolen, or otherwise fraudulent, credit card number. The merchant will often also be asked to include extra charges, such as shipping, only later to be requested, by the fraudster, to have the difference wired back. Merchants are often confused when they see charge-backs from processing such sales, because they usually obtain an on-line authorization at the time the transaction was processed. Unfortunately, an authorization is only confirming that the card being used is active, and has the available credit, for what is attempting to be charged; "authorized" should never be confused with, "valid." The following are good indications that a charge is related to a scam: 1) Card-holder contacts the merchant via TTY (hearing impaired relay) 2) Foreign address given for shipping 3) Express delivery requests 4) Shipping address differing from the billing address. A scam will usually posses some or all of these indicators. If the merchant experiences any of these scenarios, please advise them to contact the Risk Management group so we may offer assistance.

6. It is not unusual for merchants to issue credits on cards for returned products, or if a customer is unhappy with the services he or she received. However, it is very important that the merchant ensures that, whenever possible, the credit is issued to the *same card* to which it was charged. Failing to do so opens up the merchant to potential charge-backs for, "Credit Not Processed," especially if the card-holder is expecting to see a credit on his or her statement and does not due to the wrong card being credited. Merchants also need to make sure that any refund credited to a card will be immediately debited from his or her bank account. If the needed funds are not in the account, it is likely the merchant will have issues with TMS' Collections Department.

7. Visa/MasterCard regulations prohibit merchants from processing any transactions that represent sales to any principal, partner, proprietor, or owner of the merchant. These types of sales are viewed as a "Cash Advance" even if the merchant is rendering normal services to the card holder. When identified by Risk Management, such transactions may be placed on reserve and reversed back to the card to which it was charged. Merchants also may not sell anything through their TMS issued terminal that has not been directly approved to be sold by Total Merchant Services. Such activity is known as, "Factoring" and when identified, may be cause for TMS to terminate the contract with the merchant. Generally, if a sale is outside a merchant's normal business operating procedure, it's always better for that merchant to take another form of payment.

8. Many businesses, especially those which provide specialty or custom-order products, need to take an up-front deposit in order to have the capital to place the order with their suppliers. However, when advance payments are taken by credit card, the acquired funds are not certified, and are easily retrieved by the card-holder, should he decide to cancel the services before they have been rendered. If a card-holder has not been provided with ***one hundred percent*** of the requested product, that person has the ability to charge-back any given deposits for, "Services Not Rendered." If such a dispute is made, the merchant must provide written documentation to the contrary, in order to win such a charge-back. Many merchants believe that no such risks exist, due to the signed agreements most of them obtain before placing such an order. However, any such contract will not protect the merchant, should the card-holder dispute the deposit, because the charge-back rights of the card-holder supersede any agreement, verbal or written, a merchant may have with his or her customer. Deposits taken by credit card are subject to being held in the merchant's reserve account, until proof of job completion can be provided to the Risk Management Department.

9. Merchants with negative processing history may have been added to a listing known as, "MATCH" (Member Alert To Control High-risk). Before setting up an account, it is a good idea for Sales Partners to inquire about any prior processing a merchant might have had, and if any such agreements were terminated by an acquiring bank. Total Merchant Services does not cross-reference applications against the MATCH list until after accounts have been approved. Knowing about previously terminated merchant agreements in advance may save a Sales Partner a good deal of time and effort, as new accounts which are identified as being on MATCH are usually immediately terminated by Total Merchant Services.

10. Surveying the site of a business is one of the primary duties of a Sales Partner when setting up a new account. Every so often, the Total Merchant Services' Risk Management department will request a review of the business location from a third party. These requests are generally made on businesses that have limited processing, or negative credit history. Such Site Surveys are usually unobtrusive, with only a few simple questions being asked of the merchant, along with a few pictures being taken of the location's inventory and signage. These appointments are normally scheduled in advance, and during a time that is convenient for the merchant. Failure to comply with these inquiries may lead to Risk Management terminating the merchant's processing agreement.

If you have any questions, please contact Risk Management at (888) 514-0048, Ext. 9401 or by email: RiskManagement@MerchantServicesHQ.com

Wishing you continued sales success,

Risk Management