

white paper

RISK
MANAGEMENT

PRESENTED BY THE
RISK & FRAUD
MANAGEMENT COMMITTEE
OF THE ELECTRONIC
TRANSACTIONS
ASSOCIATION

Volume 2 Issue 1
April 17, 2006





Risk Management White Paper

ELECTRONIC TRANSACTIONS ASSOCIATION
2005-2006 RISK & FRAUD COMMITTEE

Mary Dees Griffith (Chair)

President
creditranz.com
5068 West Plano Parkway, Suite 300
Plano, TX 75093
(972) 392-7594
mdees.griffith@creditranz.com

Jeffrey Beene (Vice Chair)

Executive Vice President / Chief Compliance Officer
Pipeline Data Processing, Inc.
4400 North Point Parkway, Suite 190
Alpharetta, GA 30022
(678) 325-2602 x101
jeff.beene@pipelinedata.com

Barrie Berman VanBrackle

Partner
Mannatt, Phelps & Phillips, LLC
1501 M Street, NW
Washington, DC 20005
(202) 463-4330
bberman@manatt.com

Mark Cook

Vice President, Risk Management
TransFirst LLC
371 Centennial Parkway
Louisville, CO
(303) 402-8169
mcook@transfirst.com

Jeffrey D. De Petro

Vice President, Credit, Risk & Chargebacks
EVO Merchant Services
51 E. Bethpage Road
Plainview, NY 11803
(516) 962-7849
jdepetro@goevo.com

Stephanie Gibbons

Fraud Manager
Authorize.Net
915 South 500 East, Suite 200
American Fork, UT 84003
(801) 492-6515
sgibbons@authorize.net

Laurie LeBoeuf Novacek

Senior Vice President
Merchant Choice Card Services
16211 Park Ten Place
Houston, TX 77084
(281) 579-4438
lnovacek@deltacard.com

Eduardo Perez

Vice President
Corporate Risk & Compliance
VISA U.S.A., Inc.
P.O. Box 8999
San Francisco, CA 94128-8999
(650) 432-2375
edperez@visa.com

Steven Peisner

Vice President
Acquiring Solutions International
23875 W. Ventura Blvd., Suite 204
Calabasas, CA 91302
(818) 591-9099
steven@aql.com

ETA Staff Liaison

Rob Drozdowski
Senior Director
(202) 828-2635
rob.drozdowski@electran.org

TABLE OF CONTENTS

1. Executive Summary	Page 2
2. Managing Merchant Processing Risk	Page 3
3. The Shape of Fraudulent Activity	Page 4
3.1. Bait and Switch Criminal Fraud	
3.2. Business Format Change	
3.3. Merchant's Never Ship	
3.4. Factoring	
3.5. Two Card Refunds	
3.6. Long Term Liabilities	
3.7. Fraudulent Cards	
3.8. Stolen Card Numbers	
3.9. Authorized, but Unissued Card Numbers	
3.10. Forced Sales	
3.11. Re-Submitted Transactions	
3.12. Other Suspicious Patterns	
4. Risk Mitigation Techniques	Page 9
4.1. Volume Analysis	
4.2. Product Sold	
4.3. Business Practices	
4.4. Ghost Shopping	
4.5. Credit %	
4.6. Business Financial Review	
4.7. Guarantor Financial Review	
4.8. Reserves	
4.9. Data Security Education	
5. Merchant Monitoring Techniques	Page 11
5.1. Processing Limits	
5.2. Average Tickets	
5.3. Chargebacks	
5.4. Credits	
5.5. Batch Monitoring	
5.6. 4 D's of Monitoring	
6. Conclusion	Page 13

1. Executive Summary

This is one in a series of white papers authored by the ETA Risk & Fraud Management Committee designed to provide members of the ETA community with information regarding industry trends in managing risk within their respective portfolios. The purpose of this paper is to share information and strategies for improving risk management practices and reducing fraud in the acquiring side of the payments industry.

Acquirers are at financial risk from merchant performance in several different ways. While many industry initiatives are focused on fraud and identity theft, the reality is that a significant percentage of the financial loss associated with credit and debit payments comes from organized fraud, business failures, inadequate monitoring of merchant accounts, and financial loss from unfunded chargebacks. Acquirers need to focus on the performance and financial strength of their merchants as part of their overall risk strategy.

One of the key areas of focus for any merchant acquiring risk management program should be the subset of accounts that can cause the most harm. The higher volume processing accounts, low volume/high ticket retailers, merchants who are prone to chargeback activity, and merchants who provide future delivery of products and services can create larger losses if they incur financial difficulties. Acquirers need to have an effective review of their existing merchants on a regular basis, in addition to a thorough due diligence process for new merchants.

This paper will focus on providing the reader with an overview of the various types of payments fraud existing in the marketplace today and will examine some of the strategies and tactics organizations can consider in order to develop an effective acquiring payments risk management program.

2. Managing Merchant Processing Risk

Developing an effective merchant processing risk program is more art than science, along with a bit of intuition and good luck. There is no one set algorithm or methodology that can be used to manage transactions risk. Discovering transaction fraud may simply be the result of a hunch, and at other times it may be based on years of risk management experience. Each organization's risk profile is unique depending on many factors including merchant type, transaction volumes, technological resources, and other criteria. Moreover, any effective risk program must be dynamic and adaptable in order to combat the latest criminal tactics.

Many risk management professionals suggest adopting a "Sherlock Holmes" attitude when managing risk: the theory of deduction, or "Common Sense." One such informal approach for risk reviews and investigations can be thought of as the 50/50 rule, where 50% of the conclusion is determined by the merchant explanation, transactional data and transaction documentation, while common sense determines you the other 50%. For example, does it make sense that a merchant who sells used computers at a flea market is now contracted with a major cable company to install its entire network? However, when you have a merchant who sells "glow in the dark" light sticks, and he/she indicates that the company received a government contract to provide this product to the troops overseas, this may seem reasonable.

3. The Shape of Fraudulent Activity

There are many ways in which merchants and consumers attempt to commit credit card fraud. Consumers may attempt to cheat merchants; and merchants may try to cheat consumers and acquirers. In addition to deliberate criminal activity, there are many scenarios in which merchants and acquirers are victimized by consumer activity, such as consumers unable or unwilling to pay their credit card invoice when received, i.e. so-called “friendly” fraud. The next few sections provide an outline of some of the more common ways in which acquirers might be victimized and some of the preventive measures that can be used to mitigate fraud risk:

- 3.1. ***Bait and Switch Criminal Fraud:*** Criminals may assume the temporary identity of legitimate merchants and enter acquiring relationships for the sole purpose of committing criminal fraud. They bait the acquirer by appearing to operate as trouble-free merchants for the first several months of their relationship with the intent to fool the acquirer into thinking they are legitimate so that the acquirer will lessen its scrutiny. After a time, the merchant begins to process all types of fraudulent transactions, including illegally obtained card numbers, and card numbers submitted by friends, employees or collaborators with plans to chargeback the transactions. The merchant will receive the funds and disappear, leaving the acquirer to suffer the loss from chargebacks.

Preventive Measures: Prevention of this form of fraud is aided by careful underwriting before an account is approved, including reviewing records of the merchant’s previous processing history with other acquirers, obtaining references from the merchant from other vendors and conducting a thorough company background investigation. If the merchant is new, setting proper contingency reserves is an important risk management strategy. However, payments professionals need to exercise caution, as fraud will often appear before a significant amount of reserved funds have been accrued. In addition to the investigation before signing the merchant, careful ongoing monitoring might detect sudden changes in transaction patterns. Some examples of potential early indicators of fraud include: earlier than normal chargebacks, higher credits, negative daily settlement amounts, or an increased difficulty in reaching the merchant by phone.

- 3.2. ***Business Format Change:*** Merchants who cannot get approved to sell certain types of high-risk services or merchandise, or who might be denied a merchant account because they operate using a business format that is risky (such as multi-level marketing) often obtain merchant accounts by lying about the nature of their product or their business practices. They are classified by the acquirer as one type of merchant, but then engage in a different business than what they indicated on their application. Sometimes the difference is subtle, such as a travel agent who begins selling certificate travel programs, or an on-line newsletter publisher who starts to sell financial service products. Other times, the change is quite stark – from saying that they are selling a newsletter for pool owners to suddenly operating an adult site.

Preventive Measures: The fraud could be detected via random customer contacts and ‘ghost’ shopping. Additionally, transaction monitoring techniques that analyze average transaction values, transaction patterns, chargeback reason codes, and chargeback volume/timing are effective at combating this type of fraud. For example, if a merchant typically sells a variety of merchandise, the value of the tickets should be varied by product price and quantity. If the transactions soon become smaller, say \$29.95 and these occur on cardholder records once a month, it may indicate a subscription or time payment has been sold, possibly for an adult internet site. Depending on the product they are truly selling, look out for monthly processing that exceeds expected sales or an increase/decrease in returned sales (credits). As in many of these fraud scenarios, one of the most effective means of detection is random interviewing of cardholders and for risk managers to pose as customers to see if the merchant is selling what he said he would (‘ghost’ shopping).

- 3.3. **Merchant’s Never Ship:** Merchants may process transactions and never ship the merchandise, or ship deliberately defective or incomplete products. The merchant may not honor a chargeback request and leave the acquirer to take the loss.

Preventive Measures: The most effective means of detection is random interviewing of cardholders to see if they have received the product/service and that they are satisfied with the merchant. Risk managers can also pose as customers to see if the merchant is selling what he said he would. Also, in some cases, it is necessary to ask the merchant randomly for receipts from shipping companies proving delivery.

- 3.4. **Factoring:** Merchants sometimes accept transactions from a third party vendor. They do this because the third party vendors cannot otherwise obtain a merchant account on their own. Typically, the other vendor offers to compensate the legitimate vendor if he allows his merchant account to be used to process transactions. The transactions have not been consummated with the original merchant, nor do the cardholders know or realize who the original merchant is, as they are only familiar with the third party vendor. Either or both the merchant and vendor may be fraudulent.

Preventive Measures: This form of fraudulent activity is specifically prohibited by the card company operating rules. Detection is possible by careful underwriting and risk monitoring, which should reveal different ticket amounts than expected and different patterns of purchases. Random customer calls, reviewing cardholder chargeback documentation, and “ghost shopping” are methods that should reveal the fraud.

- 3.5. **Two Card Refunds:** A merchant sometimes runs a debit on one card, then credits for a dollar amount slightly less than the original amount on another card. This is one method that can be used for laundering money. It also is a method used to defraud acquirers since the merchant would be paid for the processing and then, through the friendly third party’s cards, also receive the credits. Until recently, this practice was most typically associated with credit card transactions, however today, credit is also being provided through offline debit cards. The third party then withdraws the funds via a bank or ATM, making the reversal/return of the fraudulent credit difficult.

Preventive Measures: This can be prevented, in part, by establishing a policy of no credits back to a card other than the card originally debited. In addition, risk managers may be able to detect and monitor accounts for an unusual increase in credit amounts.

- 3.6. ***Long Term Liabilities:*** The greatest losses most acquirers experience are from long-term liabilities created by a merchant. For instance, a merchant who provides Internet access for \$100.00/year and, after only providing three months of service to its customers disappears. Because the life of the service was for a year, the cardholder can charge back the transaction in the fourth month, since part of the service that they paid for will never be fulfilled. The merchant has received the funds from the sale, leaving the acquirer to take the loss.

Preventive Measures: This can be prevented, in part, by establishing a policy that restricts merchants to a maximum 90-day product/service billing cycle (i.e., billing a cardholder \$25.00/quarter instead of \$100.00/year). This strategy also minimizes the exposure due to the reduced transaction size.

- 3.7. ***Fraudulent Cards:*** Consumers and/or merchants may attempt to defraud acquirers by knowingly submitting transactions using fraudulent credit cards.

Preventive Measures: Some ways to detect this type of fraud is by monitoring the number of authorization attempts. When an authorization is not obtained for a specific dollar amount a second attempt will often be done for a dollar amount less than the original amount, and so on until an authorization is obtained. Additionally, multiple transactions to the same card are also an indicator of potential fraud. The time between transactions can also be a potential fraud indicator. For instance, if a sale is processed for a camera at 1:00pm, a second sale is made at 1:15pm, and then another at 2:00pm this may be an indicator of consumer or merchant fraud. How are the multiple sales explained? Many fraudulent merchants will say that the consumer left the store and came back to purchase more merchandise. This is suspect behavior that should be investigated by requesting copies of the sales draft.

- 3.8. ***Stolen Card Numbers:*** Criminals occasionally get a hold of a valid card or card number and use it before it is reported as stolen by the legitimate cardholder. The criminals often first attempt a transaction for a small amount to see if the sale goes through. Once it does, they will continue to run sales, each for a higher amount than the last until they are unable to obtain an authorization or someone catches on. Additionally, if there is more than one individual involved in the fraud, the valid card may be shared among multiple perpetrators, each running transactions on the same card.

Preventive Measures: This kind of fraud sometimes can be caught during the authorization process, or by comparison of the numeric address (ZIP code and numerals of the address) submitted by the card user against the known address information on file at the card's issuer – i.e. Address Verification Service (AVS). Also, it may be possible to detect the use of fraudulent cards by noting repeated uses of the same card, sale amount patterns and other pattern recognition techniques.

- 3.9. **Authorized but Unissued Card Numbers:** There are millions of card numbers that are assigned to an issuing bank in certain sequences, which have not been issued to a cardholder. If submitted for authorization, these card numbers will appear valid – as they are not listed as lost or stolen – and may receive an authorization through one of the credit card networks unless the card record is submitted for full credit authorization to the issuing bank. Additionally, there are software programs that use an algorithm to generate numerous authentic card numbers in a sequence. Once obtained, the numbers are attempted until a valid number is accepted. Many times, the criminals will use a computer program to automatically submit card numbers to a merchant until they find numbers that will survive the merchant’s authorization process. These card numbers are then used by the criminals themselves, or sold/traded for cash.

Preventive Measures: This form of fraud can be difficult to detect and can result in substantial losses unless sophisticated computerized pattern recognition algorithms are utilized. Such fraud may also be detected by risk management procedures that examine card number submission patterns, including noting the frequency of submissions from the same geographic area, phone number and other factors. In some cases, the criminal is careless and submits card numbers with the same BIN numbers repeatedly. Risk managers should also be on the lookout for the use of sequential patterns that can be easily spotted, as the last few numbers will differ only slightly.

- 3.10. **Forced Sales:** If a merchant cannot receive a valid authorization for a sale of a certain amount, say \$500, because the cardholder appears not to have enough credit available, he may attempt to re-submit the sale repeatedly, at ever lower values, until the sale is authorized.... \$450, \$400, \$350 and so forth. Or, the merchant might wait several days or weeks to re-submit the transaction, hoping that he will find a moment when the credit balance has been restored to the card. The problem with these transactions is that the cardholder did not agree to the sale amount and could dispute the charge when invoiced.

Preventive Measures: This form of merchant fraud sometimes is detected by automatically screening transactions for multiple authorization attempts on the same card.

- 3.11. **Re-submitted Transactions** If a merchant has transactions that are declined because they are fraudulent, or otherwise blocked by fraud screening (for instance, if the AVS does not match) he might attempt repeatedly to resubmit the card over a period of days, weeks or even months, until he finds a moment when the card might slip through the system.

Preventive Measures: This form of merchant fraud sometimes is detected by automatically screening transactions for multiple authorization attempts on the same card.

3.12. *Other Suspicious Patterns Include:*

- Average tickets exceed the maximum ticket allowed
- Daily/weekly deposit amounts exceeding the maximum limit
- Multiple authorizations to a card exceeding maximum
- Number of declined authorization attempts exceeding maximum
- An unusual pattern of duplicated card numbers appearing in batches
- An unusual frequency of same dollar amounts appearing in batches
- Same card number appearing over a period of time in both swiped and keyed transactions
- An unusual frequency of even dollar amounts appearing in batches
- The batch is in an even numeral dollar amount
- Credits exceed debits in the batch
- There are an unusual number of voids and credits in batches

4. Risk Mitigation Techniques

Some acquirers conduct “*high risk reviews*” by a risk committee in the same way a credit committee may be used to approve accounts. The focus of these risk reviews is to better assess merchant performance and financial activity. While the frequency of the review may vary from merchant to merchant, a good approach is to review well performing accounts annually, and underperforming accounts quarterly, monthly, or when the account has surpassed the merchant monitoring criteria. Most reviews include the following:

- 4.1. **Volume Analysis:** If a merchant’s volume increases 25% or more unexpectedly, it may be necessary to contact the merchant to understand why the volume has increased. Usually, it will be due to unexpected growth of their business. In most cases, it is desirable to re-underwrite the merchant to ensure the volume increase will meet your credit criteria and expectations.
- 4.2. **Product Sold:** It is important to understand what products and services a merchant is selling. If an acquirer observes a change in the average ticket value (e.g., volumes, credits, etc.), this may be an indication that the business plan has changed and the merchant may be selling a different product or service.
- 4.3. **Business Practices:** If a merchant sells a product or service that will not be shipped or provided until a future date, this will add time liability to the transaction. Various regulations allow cardholders to dispute transactions (chargeback) for goods or services not received. Pursuant to the card company rules/regulations, many of the timelines associated with these chargeback rights do not start until after the expected delivery date of the product or service. For example, if a merchant states in the promotional material “Please allow 4-6 weeks for delivery”, the chargeback rights for that transaction do not start until the day after the 6th week from the transaction. This will add additional liability to the merchant’s processing. Acquirers need to assess the overall risk for the merchant account based on when the merchant fulfills the order. In the example above, some merchants will not bill the cardholder until the date of delivery of the product or service, which eliminates the additional timeframe risk.
- 4.4. **Ghost Shopping:** Ordering products or service can provide a genuine indication of how a merchant performs. If the merchant states a product or service will be shipped in 2 days, and the actual delivery time is 3-4 weeks; it may help understand what challenges the merchant has in reducing chargebacks due to non-fulfillment.
- 4.5. **Credit %:** Monitoring and reporting on a merchant’s credit percentage vs. their monthly volume may be an indicator of the quality of the product/service sold. It also may be a gauge for the level of chargeback activity increase that may occur if the merchant were to close or file for bankruptcy protection. While the percentage of acceptable credits will vary from merchant to merchant, credit percentage above 10-15% is considered excessive (though some direct marketers, catalogue merchants, and Internet merchants have credit percentages over 30%). This type of analysis is supported by effective “know your customer” techniques.

- 4.6. **Business Financial Review:** The business financial review is generally based on cash flow, asset review, and the overall value of the business. The combination of these three elements, as well as other factors, will help assess the overall financial strength of the business. Analyzing cash flow is important to ensure that fees and chargebacks will be honored when presented to the operating account. Positive cash flow is essential for merchants who conduct future delivery of products and services. A thorough asset review will help determine the ability of the merchant to conduct business. Acquirers should ensure that there is adequate cash, inventory, and tangible assets to sustain the merchant activity. Another key evaluation criterion is the net worth of the business (retained earnings) which is a good indication the overall financial health of the business. Analyzing the value of the business, the liabilities, and the net income help in the understanding of the financial risk compared to the operational risk of the business.
- 4.7. **Guarantor Financial Review:** Understanding the net worth of a personal guarantee will help determine if the guarantee is a strong mitigating factor to the risk of the account. Personal guarantor accounts that have a solid asset base tend to perform better too. Guarantors that are generally well established in their community are less likely to commit fraud, skip out, or not cover their merchant processing obligations.
- 4.8. **Reserves:** Once an acquirer or processor understands the risk associated with a merchant account it is important to ou should weigh the strength of business financials and personal financials (if applicable) to determine the overall risk. To mitigate risk further, should consider establishing a reserve account. Merchants can fund reserve accounts with up front cash, letters of credit, or fund the reserve over time from daily merchant deposits. Reserves are a great way to mitigate risk exposure and allow an acquirer to accept an account they may not otherwise approve. Knowing how much to reserve will depend on the comfort level with the account. Many acquirers fund reserves with a percentage of daily deposits (e.g., 3%-10%) over a period of time. This is called a rolling reserve. Merchant accounts with reserves require continual analysis to ensure that monthly reserves are adequate for the additional risk associated with the account.
- 4.9. **Data Security Education:** When an assessment of the merchant is complete, it is important to educate merchants about the importance of data security and applicable legislation and compliance mandates. Safeguards should be put in place to protect the personally identifiable information of consumers and mitigate the risk of a data compromise. Moreover, many states have implemented data notification laws in the event a consumer's personally identifiable information is exposed, and it is important that merchants understand their responsibility pursuant to state law. In addition to federal/state legal requirements, the Payment Card Industry's Data Security Standard ("PCI DSS") defines a standard of due care for protecting cardholder data for any entity who stores, processes, or transmits cardholder data. For more information:
- State Data Security Laws: www.electran.org/info/industry_info.asp
 - Visa www.visa.com/cisp
 - MasterCard www.mastercard.com/us/merchant/security
 - American Express www.americanexpress.com/fraudinfo
 - Discover www.discoverbiz.com/resources/data/data_security.html

5. Merchant Monitoring

The risk department is responsible for monitoring the merchant's processing to guard against fraud and loss. The monitoring not only protects the company but also protects the merchant from possible fraud and loss. Additionally, through the monitoring process, customer service and training should be provided to the merchant. This enables the merchant to process positively with the additional knowledge and training provided by the risk department.

The risk department monitors the merchant's processing based on certain criteria and patterns. Some of the more common monitoring criteria include:

- 5.1. **Processing Limits** – The merchant is granted a monthly processing limit. This limit allows the merchant to accept credit card transactions up to that approved limit. The merchant's processing volume is monitored throughout the month to ensure the limit is not exceeded.
- 5.2. **Average Tickets** – During the merchant account approval process, an average ticket is calculated. This is the average of the prices of the product or service offered by the merchant. Any transaction that exceeds the average ticket is investigated.
- 5.3. **Chargebacks** – The number of chargebacks, percentages and reason codes are monitored to ensure compliance with card company rule and regulations. This allows for the profiling of a merchant's processing and business practices which in turn allows the risk department to work with the merchant to reduce chargebacks.
- 5.4. **Credits** – Credits are monitored to gauge possible loss. The credit percentage and dollar amounts are monitored to ensure compliance with all rules/regulations, and that credits are being performed appropriately to reduce the potential for unnecessary chargebacks. This also ensures that fraudulent credits are not issued. Credited transactions are also forecasted in the event a merchant declares bankruptcy. Combining credits and chargebacks, an acquirer can estimate how much reserve may be needed to cover any potential loss.
- 5.5. **Batch Monitoring** – After each day's processing the risk department will monitor each batch submitted. Numerous items are reviewed, including but not limited to, transactions that exceed the average ticket, excessive authorizations, credit and chargebacks, proper usage of AVS and correct CV code acceptance just to name a few.
- 5.6. **4 D's of Monitoring** – One approach to remembering the key factors of risk monitoring is to consider the "4 D's of Monitoring:"
 - Data
 - Document
 - Dial
 - Delivery

D1 – Data

Review the transactional data. Was the transaction swiped or keyed? Did the merchant obtain positive AVS or CV code? Was a valid authorization obtained? Were there multiple authorization attempts?

D2 – Document

Request a copy of a document (sales draft) from the merchant. Review the document for validity. Is the charge correct? Is the charge full payment, a deposit, or a split sale? Did the cardholder sign the document? Is there any long-term liability? What are the shipping procedures? Did the merchant get signed delivery confirmation?

D3 – Dial

Request a “dial” to be performed. A dial is just that, a call dialed to the cardholder and/or Issuing Bank to verify the transaction. Sometimes it is good to get the merchant involved. Request that the merchant have the cardholder contact the issuing bank to provide fulfillment on the dial request. Upon receipt of the dial verification, act accordingly. Note the file with the dial results. Contact the merchant, provide results and inform them of the next action (i.e., release of funds, credit, further holds, etc.).

D4 – Delivery

Request a delivery confirmation from the merchant if the sale was not “cash and carry”. Perform a dial for delivery confirmation from the Issuing Bank and/or cardholder. For certain, business types, acquirers might be forced to require the merchant to request a signed delivery confirmation when shipping product. These business types may include, computers, electronics and full furniture suites to name a few. The requirement for a signed delivery should be discussed internally and then be required of the merchant if determined that it is needed.

During the monitoring process, exception items are investigated based on certain risk criteria. Once the issues are identified, the merchant is contacted and issues are discussed. In working with the merchant, the issues discussed may range from requesting a copy of a transaction to analyzing and preparing a chargeback reduction plan. An effective risk management program will include documentation of the issues and outcomes in order to develop a merchant history.

6. Conclusion / Summary

The key to any effective risk management program is follow-up. Once a merchant is identified as a concern, there is usually additional work to be done. A remediation plan may include obtaining additional information, implementing chargeback reduction plans, obtaining updated financial statements, and possibly increasing reserve requirements. In almost all cases a detailed conversation with the merchant is necessary.

The value of a risk management plan is to mitigate the financial exposure to the acquirer. This is done through improved processing performance, or increased reserves if the merchant continues to under perform. In most cases, if the merchant understands the financial risk involved, they will appreciate the need for an acquirer to mitigate transactional risk.