

# The Merchant Account Risk Management Report

## "How To Easily Stop eCommerce Fraud And Increase Your Profits"

By Paul Nisenbaum  
The ePaymentGuru  
Merchant Account Consultant  
[www.ePaymentGuru.com](http://www.ePaymentGuru.com)

**Dear '123 Gift for Me' Participant,**

(Note: Since you downloaded this report from '123 Gift for Me,' don't forget to look for the bonus at the end.)

Imagine waking up one morning, strolling into your home office, hit your "check email" button and... **there are NO orders!**

Even on a bad night you would get at least a couple orders. Something is wrong, but your website is up. The order form is there, but when you test it out, the order is declined, giving some cryptic decline code.

You call up your merchant account provider to find out why your orders are being declined and after a 30 minute wait you finally talk to somebody... and they can't help you, but give you another department to try.

Finally you reach Mr. Fox in the "risk department," who coolly tells you,

"We're investigating your account because you have sales than normal."

You sputter, "What?"

Mr. Fox continues, "So until we have finished investigating your account, you can **no longer process transactions**. And the past weeks worth of sales are not going to be deposited into your account until this is finished. We'll send you a letter that will tell you this took place."

You shake the phone and try not to scream, "What do you mean that I won't be able to process transactions? For how long?"

Mr. Fox replies, "Humm... it looks like the investigation may take 1 to 4 weeks."

You stutter, "Four..rrrr weeks?"

Again Mr. Fox, ". . . and those funds will be held for 6 months just in case of future problems."

It's a nightmare, a weeks worth of sales is now being held ransom, yet you still have to pay the marketing and product expenses for them. And you have no way to take any new orders.

### **You are out of business!**

I'm sure you are thinking, "That would never happen to me. I am an honest trustworthy person."

Unfortunately, to your merchant account provider you may be just another account number and a risky one at that.

And in fact, their Risk Department may think of you as the enemy because you may cause them to lose a lot of money.

It doesn't have to be that way.

### **You should never have to worry about the most critical part of your business - getting the money.**

With the information in this report you can take a step forward to making sure you do not become the next horror

story. And in fact actually put more money into your pocket every month.

### **In this report you will learn...**

- **Reasons why you could "get into trouble".**
- **How to make you and your business "horror story proof"** so you **never** have one of those all too common experiences.
- **How to stop fraudulent orders and chargebacks.** Including the top types of fraud orders you will see, how to identify them, and prevent them to reduce your risk of chargebacks.

### **Reasons why you may "get into trouble":**

- Your merchant account contract has maximum dollar amounts for both monthly sales volume and sales prices, in addition to types of products/services sold.
  - If you exceed your limits or change products, the Risk Department will see this as an increased risk. Their job is to make sure that the provider does not get saddled with costs if you, the merchant, cannot pay the costs for returns or chargebacks.
  - When you signed you up for your merchant account you may not have been aware of these issues or you didn't read the fine print or the sales person did not give you a full explanation.
  - After you signed up for your merchant account, nobody followed up with you to help you monitor your sales or products and/or you may have forgotten about these limits.
- You have a number of fraud and chargebacks (fraud problems will result in chargebacks)

## How to "stay out of trouble" and horror proof your account:

- **Communication, Communication, Communication.**
  - Find a merchant account provider that understands online businesses and provides support with real people via phone and email.
  - Work with your merchant account provider to **proactively help you before and after you setup your merchant account.**

Periodically review your account limits and products stipulated in your contract. Send an email or letter, and then phone your provider ...

- When you will exceed your monthly sales volume
- When you have seasonal increases in sales
- When you increase product prices
- When you add new products

- **Stop fraud and chargebacks.** See the next section.

## Fraudulent Orders and Chargebacks

When, not if, your Internet business has fraudulent sales you not only lose money and products, but you lose time. Since dishonest people are always trying to find ways to steal, you must be on guard 24/7.

As online business owners, we are particularly vulnerable to fraud since we take orders without actually seeing our clients and without swiping their credit card.

In addition, if you sell downloadable products, then the fraudster can use a stolen card number, receive the product, since it is delivered immediately, and then the real card holder may file a chargeback claim against you because an order was placed on his compromised card.

If you have too many chargebacks, VISA and MasterCard may have your provider lock or close your account.

## **The Two Most Common Frauds are Dishonest People That:**

1. **Use stolen cards to purchase your products.** Cards are physically stolen or via phishing computers connected to the Internet. The card information is then sold online to other fraudsters.
2. **Order, and then claim they never received your product.** They ask for a refund or file a chargeback claim.

## **Proven ways to prevent fraud:**

Review and implement the following fraud prevention strategies and I guarantee your fraud and chargebacks will dwindle.

### **Accept "Terms Policy"**

Before a purchaser can complete their order, display your Terms Policy with a check box to Accept Terms.

Alternately, have an easy navigation to/from the Accept Terms statement.

### **Address Verification Service (AVS)**

Always use AVS as it requires the client's billing information associated with his credit card to match the information he ordered with (same address for example). Presumably, a thief will not necessarily know both the name and correct zip code. AVS is available from your merchant account provider.

**Fraud Prevention Policy** - You can state that to prevent fraud that you actively review all sales and call clients if necessary.

**Guarantee / Refund Policy** - Plainly state your guarantee and refund policy. Make sure you have a straight forward

way for a purchaser to get a refund. **It's always best to give a purchaser a refund to prevent or diffuse their anger.** Angry people may try to harm your business, spread rumors, and file chargebacks.

### **Billing vs. Shipping Address**

If the billing address is in Texas and the shipping address is in Florida or Romania or a post office box, give the card holder a call before shipping the product.

### **Billing Address vs. Contact Phone Number**

If the billing address is in Detroit and the contact phone number is in New York City, call the number and ask questions. You can also use a reverse lookup to find out the billing name for the suspected phone number.

### **Billing Address vs. IP Address Location**

Ask your merchant provider to alert you if a client's IP Address is not in the same location as the billing address (especially if not in the same city or country).

### **Chargeback History**

Ask your merchant provider to alert you if a client has a history of chargebacks.

### **Merchant Name and Phone Number on Credit Card Statement**

When a purchaser reviews his monthly credit card statement, he should easily recognize the name of the merchant of a purchased item; otherwise he may file a chargeback. Hopefully, if he sees a merchant phone number next to the item, he will call the number before calling the card company and requesting a chargeback.

Actually, this happened to me. I was reviewing my MasterCard statement and I saw an item for \$99 and I did not recognize the merchant. I called the number beside the name and found out that I knew the merchant. I told her that she needed to put her company name on the statement to avoid problems.

### **Multiple Orders**

- Fraudsters try fishing for a valid credit card number by ordering many times, changing a number or two. This works the same way as scammers try to find valid passwords.
- Other times, thieves will use a stolen credit card rapidly before the card is shutdown.
- Sometimes when someone orders online, they click on the order button a couple of times because they aren't sure that the order went through the first time. This can happen if the Internet itself is slow or their Internet provider is slow or their computer is slow. You can add a little note next to your order button to only click on it once.

### **Large Orders**

Thieves will use a stolen credit card for purchasing a lot of items before its shutdown. This scheme also applies to the Billing Address vs. Shipping Address scam.

### **Email Addresses**

Thieves sell credit card numbers and even the complete AVS billing address for that credit card to other thieves. Some thieves will just make up names and email addresses to use when placing these orders.

**Free email Addresses** - Since scammers use free email addresses (Hotmail, Yahoo, etc.) that don't require a credit card or identification, you may want to pay special attention to those sales from those clients.

**Suspect Email Names** - Watch for email names that don't add up. For example, fake addresses may use all capital letters or a name that would be impossible to get.

BOB@YAHOO.COM or BGates@hotmail.com.

**Email address that use the person's first and last name at yahoo or hotmail.** Such as Barbara Ohlson with the email address barbaraohlson@yahoo.com or Roscoe Jones with the email roscoejones@yahoo.com (NOTE: This is

also commonly used for legitimate orders too, so do not assume an email address like this is fraudulent, it just has a higher probability.)

**English sounding name at a free email address, but the email address isn't a regular word.** For example:

Bonnie Barnes perjakajoko@yahoo.com or  
DAN PHAN anakbawangku@yahoo.com

**Part of the order is in all caps such as the address, but the name or email address is all lower case (or vice versa).** That is because the stolen information purchased was in all upper case which they copy and paste into the order form and then type in a name or email address.

**If you have suspicions about an order,** call or send them an email letting them know you occasionally check orders to make sure that the person placing the order is also the card holder and have them verify their order.

### **Rapid Delivery**

For physical products, be alert for orders that require overnight delivery. Thieves want to pay for and receive merchandise rapidly before being caught

### **Proof of Delivery**

Whenever possible, obtain proof of delivery for your products. It is a bit more challenging for downloadable products. You may want to have a special bonus promotion. In order to receive the bonus offer, the client must locate a code found on page xx of the downloaded product, and type it in on the bonus offer form.

### **Keep Records**

Keep records of all contacts that you make with clients. These records will help show that you were using proper security procedures and attempts to contact the rightful purchaser.

### **And finally...**

Remember, if the order smells fishy, contact the purchaser, hopefully before fulfilling the order. If you can't make contact, you can cancel, void, or refund the order.

## Conclusion

Okay. You learned many ways to reduce the risks with your merchant account.

- Find a merchant account provider that understands online businesses and provides support with real people via phone and email.
- Proactively communicate with your merchant account provider about increases in your monthly sales volume, product pricing, and products.
- Implement proven ways to stop fraud and chargebacks.

When you take action on these issues, you will reduce fraud, chargebacks, save time, which we all know will easily increase your profits.

Cheers,



Paul Nisenbaum, the ePaymentGuru

[www.ePaymentGuru.com](http://www.ePaymentGuru.com)

For a free 15 minute consultation or just for more information, send me an email [paul@ePaymentGuru.com](mailto:paul@ePaymentGuru.com)

**Bonus...** since you downloaded this report from '123 Gift for Me,' when you sign up for a merchant account through me, you won't have an annual fee, ever, and you'll get a \$25 discount on the setup fee.

In order to receive the special pricing, just let me know in an email or use the following link to see fees and apply online (no obligation):

[www.ePaymentGuru.com/specialFeesApplication.html](http://www.ePaymentGuru.com/specialFeesApplication.html)