



Avoiding Online Fraud

Copyright and Trademark

© 2011 MonsterPay NV. All Rights Reserved. MonsterPay and the MonsterPay logo are registered trademarks of MonsterPay NV. Designated trademarks and brands are the property of their respective owners.

Notice of Liability

The information in this pack is distributed in an “as is” basis. All information provided in this document is provided with good will. The authors and publishers of this manual are not responsible for loss, or purported loss due to any contents of this publication.

Summary of Revisions

Version	Date	Changed By	Changes Made
1.0.0	01 Sep 2008	B Dos Santos - Setcom	Original document created
1.0.1	12 Jan 2009	D Liu - Setcom	Added Revision history and reformatting
2.0.0	02 Nov 2009	D Liu - Setcom	Formatted for MonsterPay

Protect your Business

The following best practices, taken from various experts, are offered to help you avoid being victimised by internet fraud. Experience suggests that there are certain characteristics that can be tip-offs to possible fraud. Each of these characteristics by itself is very seldom cause for alarm. It is usually when several of these factors characterise an internet purchase that you may be the target of a fraud scheme.

Be alert for transactions with several of these characteristics

1. Incomplete information: Begin taking a few extra steps to validate each order. Don't accept orders unless complete information is provided (including full address and phone number - do not accept cellular phone numbers only).
2. First-time shopper: Criminals usually hit a merchant once and don't go back a second or third time.
3. Larger-than-normal orders: This requires knowledge of what a "normal-sized" order is. Because they may be using stolen cards or bogus account numbers that have a limited life span, criminals need to maximise the size of their purchase.
4. Orders consisting of several of the same item. As these items are intended for resale, having more of them increases the criminal's profits.
5. Orders made up of big ticket items. These items have maximum resale value and therefore maximum profit potential.
6. Orders shipped "rush" or "overnight". Criminals want these fraudulently obtained items in their hands as soon as possible for the quickest possible resale and aren't concerned about extra delivery charges.
7. Orders shipped to an international address. A significant number of goods from fraudulent transactions are shipped to bogus cardholders outside the country.
8. Transactions on similar account numbers.
9. Transactions on multiple cards, but the orders are shipped or dispatched to a single address.
10. Multiple transactions on one card over a very short period of time: This could be an attempt to "run" a card until the account is closed.
11. Multiple transactions on one card, but multiple delivery addresses.
12. International card number(s) used for local delivery addresses.
13. Local card number(s) used for international delivery addresses.
14. Different "bill to" and "ship to" addresses. Be wary of orders with different bill to and delivery addresses.
15. Syndicates focus their activities on enterprises specialising in certain merchandise, e.g. cell phones and computers: Their method entails phoning the specific business and ordering certain articles followed by a fax in which they give permission that a credit card may be debited. Counterfeit credit card details or stolen cards are provided and in some cases copies of the front and the back of the card are also faxed to the merchant with an ID or passport number. During the whole transaction the cardholder remains "faceless" and courier services are used to collect and deliver the merchandise. No physical delivery address is provided.
16. Hotmail or free e-mail addresses: These addresses can't be tracked back to the real owner. The customer must provide an ISP or domain based address. Try not to accept any orders originating from a free, web-based or e-mail forwarding address. Install filtering software that rejects orders coming from different free e-mail services. Since there are so many free e-mail services, how do you know if the order you receive is from one of these free e-mail services?
17. Check the e-mail address for a real IP. You may do such an address check by going to a browser and putting www in front of the domain.
18. Try this with joesmith@cyberdude.com – you will see that www.cyberdude.com puts you on the I-names (150+ free e-mail domains) homepage.
19. When in doubt call the phone number (remember don't accept cellular phone numbers only) listed on the order and confirm the order.
What precautions should you take with orders from free e-mail accounts?

20. Send an e-mail requesting additional information before you process the order.
21. Ask for a non-free mail address, the name and phone number of the bank that issued the credit card, the exact name on the credit card and the exact billing address.
22. Often you won't get a reply. If you do, verify the information.

Below are some countries that online fraud often originates from. Take as many of the above precautions as possible if you see the "bill to" or "ship to" address as any of these mentioned:

- AFGHANISTAN
- ARMENIA
- AZERBAIJAN
- BURKINA FASO
- BELARUS
- CONGO (DRC)
- CENTRAL AFRICAN REPUBLIC
- CAMEROON
- COLOMBIA
- CYPRUS
- GABON
- GEORGIA
- GHANA
- GUINEA
- EQUATORIAL GUINEA
- INDONESIA
- IRAQ
- IRAN
- JORDAN
- KYRGYZSTAN
- KOREA - DEMOCRATIC PEOPLE'S REPUBLIC OF
- KAZAKHSTAN
- LEBANON
- LIBERIA
- MALI
- NIGER
- NIGERIA
- PHILIPPINES
- PALESTINIAN TERRITORY
- RUSSIAN FEDERATION
- SUDAN
- SIERRA LEONE
- SOMALIA
- SYRIAN ARAB REPUBLIC
- TOGO
- TAJIKISTAN
- TURKMENISTAN
- UKRAINE
- UZBEKISTAN
- ZIMBABWE

Website Requirements

A cardholder using a website must be able to see the following:

1. The website must clearly indicate who the merchant is. The merchant's trading name must be displayed as it will appear on the cardholder's statement.

2. The website must clearly indicate what products and services the merchant is offering.
3. The website must clearly explain the merchant's shipping practices. The cardholder must be able to determine when merchandise will be received.
4. The total costs for products or services, including all shipping, handling and tax charges must be visible.
5. All prices must be quoted in the merchant's local currency and be clearly indicated as such.
6. The merchant's return policy must be easily understandable and accessible.
7. The website must clearly provide a customer service phone number that cardholders can use to resolve queries.

Obtain cardholder details

In addition to the details that should be captured for your normal business requirements, the following should also be captured:

1. Cardholder name, card number, expiry date and CVV2 number (the last three numbers indent printed on the back of the signature panel).
2. Amount.
3. Cardholder's name and address.
4. Cardholder's identity number.
5. Telephone number (work/home and cell phone). Do not accept cell phone numbers and postal box addresses as the only reference to contact the client. Contact the client after the order has been received to verify the contact number.
6. E-mail address (if applicable).
7. Delivery address and telephone number.
8. Recipient's name and identity number.

Verify details

Verify the names and addresses telephonically with the details captured on your system. Try to use the work telephone numbers or alternatively a home phone number. Do not use cell phone numbers to do this verification. Verify and confirm all transactions from foreign cardholders in a similar way as above.

Obtain authorisation

1. The floor limit for an e-commerce merchant is zero. Therefore authorisation must be obtained for each and every transaction.
2. The merchant must obtain the expiry date of the card and the CVV2 (card verification value) and forward it as part of the authorisation request.
3. An authorisation code is merely an indication that the cardholder is in good standing with his bank and not a guarantee of payment. It does not guarantee against chargeback's for lost or stolen cards.

Delivery guidelines

1. Use your own delivery services. Try not to outsource to another company. If it is not possible to do your own deliveries, ensure that you have a good contract with the delivery company. They have to follow your rules and procedures for delivery. If they do not comply with procedures, they should share the risk.
2. The merchandise must be delivered to an agreed upon location on the agreed upon date.

3. Deliver the goods inside a house or office. Do not deliver onto the pavement, outside a door, into a vehicle or on an empty plot.
4. Confirm the receiver's identity. Use the details captured with the order and verify with an identity document.
5. Let the receiver sign for the delivery. Do not deliver without acknowledgement of delivery. If the correct recipient is not present, do not deliver goods to relatives, friends, neighbours, employees, servants or anyone else. Proof of receipt of goods is required should the cardholder dispute a transaction.
6. Retain the proof of delivery documents for at least 6 months.

General guidelines

1. A cardholder that cannot be contacted is a risk in general. Do not accept cell phone numbers and postal box addresses as the only references to contact the client.
2. Do not accept a card that has expired.
3. All transactions must be authorised.
4. Do not add any surcharges to a transaction.
5. Write "TO" for telephone orders and "MO" for a mail order on the signature line of the transaction slip.
6. Your trading name must appear on the cardholder's statement.

If you have any questions please feel free to contact us.

Additional Information

For additional information, please contact MonsterPay's Sales Department.

Tel:	United Kingdom	+44 (20) 3051 6320
	United States of America	+1 (408) 850 6530
	South Africa	+27 (83) 913 0000

Fax:	United Kingdom	+44 (20) 7681 3303
	United States of America	+1 (408) 351 8057
	South Africa	(086) 615 1486

Email sales@monsterpay.com

Web www.monsterpay.com