ATTITUDE GROUP LTD

How to Lose a Million Dollars (or not): a merchant's guide to online fraud protection

When someone is deceptive or misrepresents the truth to get things they're not entitled to, they're committing fraud. Unfortunately, this has always been a problem for the business community.

Now, with the advent of ecommerce, merchants who trade online need to be aware of the potential for loss through fraud. Anyone who conducts online transactions is at risk, including those using osCommerce. But there are warning signs you can look out for and steps you can take to minimize that risk.

This article is relevant to anyone starting out in ecommerce or for the seasoned ecommerce merchant who wants to learn more about the risks they face.

The risk of fraud shouldn't scare you off ecommerce. Our aim is to help you become more aware and protect yourself. If you have money, there's no shortage of people around the world who will steal it from you in any number of ways. But obviously many merchants are successful in spite of this. The key is to be aware of how your business could be threatened and reduce your likelihood of becoming a victim.

Legal stuff

We aren't lawyers or experts on online fraud. This article is designed to be an introduction for people who aren't aware of the risks, and/or how to respond to them. We urge all readers to investigate fraud risk and prevention thoroughly, and to seek expert advice where necessary.

The information contained in this document is provided 'as is' without warranty or guarantee of any kind. The entire risk as to the results and the performance of the information is assumed by the user, and in no event will Attitude Group Ltd be liable for any consequential, incidental or direct damages suffered in the course of using the information in this document.

Attitude's osCommerce Business Series

online_fraud_protection.pdf

Download from:
http://www.oscommerce.co.nz/docs

For osCommerce installation, customization and support, contact Attitude.

Introduction

Anyone conducting online transactions runs a risk of being defrauded. This article outlines specific things you can look out for and steps you can take to minimize that risk.

Overview

- Legal stuff
- How bad could it be?
- Online credit card fraud
- Other types of online fraud
- Assess your risk
- Things to watch out for
- High-risk areas
- Preventive measures
- What to do if you've been defrauded
- Conclusion
- Appendix 1: common types of online fraud
- Appendix 2: useful links

ATTITUDE

Attitude Group Ltd
http://www.attitude.net.nz

PO Box 40031
Christchurch
New Zealand 8001

Phone +64 3 982 1499
NZ Free 0800 828 848
Fax +64 3 366 1649

How bad could it be? The effects of online fraud

As a merchant, being a victim of fraud can have a range of effects on your business. These effects include:

- Immediate financial loss due to stolen stock/earnings
- Damaged reputation
- Loss of customer trust
- Loss of investor confidence
- Lowered sales
- Extra costs of time/money to manage each fraud incident
- Lowered staff morale
- Possible legal costs
- Lowered value of your stock/services
- Additional bank fees for transaction reversal
- Potential problems retaining your merchant's bank account after too many reversed transactions

Online credit card fraud

Theft of goods and services through credit card fraud is the most important form of fraud to be aware of, as online merchants are particularly vulnerable. Because you're unlikely to meet your customers face-to-face, it can be hard to know whether the credit card payment you've accepted is really from a valid customer. If it isn't, you may lose both the product and the payment. And while credit card holders usually have limited liability, merchants shoulder the full cost of a fraudulent transaction and related fees.

While most of the material in this article relates to online credit card fraud, you should also be aware of other online frauds that affect merchants.

Other common types of online fraud

Merchants are affected by many types of fraud other than credit card fraud. This section doesn't describe them all, but there are some types of fraud you should be especially aware of. You may be vulnerable to the following:

- Online intellectual property theft
- Misrepresented identity or identity theft
- Bogus emails and websites used to 'phish' for confidential data
- Pagejacking
- Advance fee scams
- Bad check scams
- Fake postal money orders
- Wire transfer fraud

For more detail about any of the frauds listed above, see appendix 1.

No matter what the scam is...

Don't feel that you have to reply to every suspicious letter or email. In most cases there's not much you can do by directly contacting a scammer. However, in some instances you may want to report the fraud attempt to the appropriate authorities.

Assess your risk

If you have difficulty answering the questions below, or if you answer 'no' or 'none', you should increase your awareness of fraud and improve fraud-related business processes.

1. What fraud prevention and monitoring procedures do you have in place?

2. Do you have a policy that outlines how the business treats the issue of fraud?

3. How much money and customer trust could you lose to fraud before your business is seriously crippled?

4. Do you let customers know that orders will be authenticated to rule out fraud?

5. Do you manually check each suspicious order/customer profile?

6. Who monitors and analyzes fraud related activity, and who follows up on suspicious orders?

7. Are relevant employees in your business aware of fraud warning signs and how to report them?

8. Do you keep records of customer transactions?

9. Do you keep records of order statistics for individual stock items/services?

10. Do you know which countries/areas are considered high-risk for online fraud?

Things to watch out for

It's important to watch for common signs of fraud. Though the circumstances below often apply to honest customers, they can also be indicators of illegal activity.

Pay closer attention to **orders** that are:

- Unusually large
- Shipping to an address that isn't the billing address
- Shipping to countries you don't normally ship to (especially if in high-risk areas)
- Shipping multiple identical items
- Unable to pass an address verification process
- Out of the ordinary in any way

Pay closer attention to **customers** who:

- Use an anonymous/free email address (like hotmail.com)
- Supply a non-existent or under-construction website address
- Use a disconnected or changed telephone number
- Supply a fake-sounding physical address (such as 123 Side Street) or only a post office box number
- Want shipping as quickly as possible at any price
- Do not pass credit or identity checks
- Don't make immediate full payment
- Are first time buyers

Pay closer attention to **credit card numbers** that:

- Generate multiple orders over a short time span, especially if each order ships to a different address
- Are one of several card numbers shipping to the same address

High-risk areas for online fraud

The countries/cities on the following list are considered as high-risk for online fraud, though not every order from these areas will be fraudulent. And remember: safe transactions aren't guaranteed just by shipping to areas outside this list.

- Africa
- Amsterdam in Holland
- Belgium
- Bulgaria
- China
- Eastern Europe
- Egypt
- Ghana
- Indonesia
- Israel
- Lithuania
- Malaysia
- Russia
- Malmö in Sweden
- Nigeria
- Pakistan
- Palestine
- Romania
- Southwest Asia
- Turkey
- Ukraine
- Yugoslavia

The key is to examine orders from these areas with more caution.

Customer: Mr Dodgy
123 Side Street
Someplace, 90210
Somewhere, Nigeria

Shipping Address: Mr Dodgy
123 Side Street
Someplace, 90210
Somewhere, Nigeria

Billing Address: Mr Dodgy
123 Side Street
Someplace, 90210
Somewhere, Nigeria

Telephone Number: 1234567890
E-Mail Address: dodgy@anonymous.email.com

Payment Method: Cash on Delivery

Products	Model	Tax	Price (ex)	Price (inc)	Total (ex)	Total (inc)
50 x Woollen Sweater		0%	**$45.00**	**$45.00**	**$2,250.00**	**$2,250.00**

Sub-Total: $2,250.00
Table Rate (Best Way): $8.50
Total: **$2,258.50**

Date Added	Customer Notified	Status	Comments
01/12/2006 16:12:24	✔	Pending	I need this very quick Can you ship today

Preventive measures

You don't want to scare customers off with too much red tape, but you do want to safeguard your business by establishing some basic fraud prevention measures. There's a lot you can do, but make sure you maintain a balance between keeping your business safe and keeping it customer-friendly. And remember - no single technique will make your business fraud-proof.

Shipping

- Use postal insurance
- Use package tracking services
- Use a trusted courier that requires the recipient's signature on delivery
- Suspend the delivery if you become suspicious of fraud
- Don't offer shipping to high-risk areas
- Don't ship an order until additional identity and payment checking is complete

Orders

- Validate all the details of each order
- Keep records of order statistics so you can build up a picture of typical orders
- If you've identified patterns of fraud, make sure alerts are triggered when an order fits the pattern

Customers

- Make sure the customer genuinely exists
- Keep records on customers with good purchase histories and on those you've had trouble with
- Use a means such as AVS (Address Verification System) to make sure the customer's physical address is valid
- Make sure both the billing and shipping addresses are valid, especially if they are different
- Keep records of all contact you have with customers
- Use a means such as online phone books to check that a supplied phone number is valid
- Ensure any email or web addresses are valid and reputable
- Ring the customer to verify their order
- Make it clear to all customers that orders and payments will be authenticated before shipping
- Warn customers that their transaction details and their IP number (Internet address) will be recorded
- Keep records of customer purchases to establish their typical buying patterns

Credit cards

- If in doubt, ask for an independent copy of the customer's signature
- Ask the customer to fax the front of their credit card
- Keep a record of credit card numbers you've had problems with or suspicions about in the past
- Find out the card's issuing bank and country of origin and make sure they match the information you've been given by the customer
- Use a means such as CVV2, SecureCode or CID (depending on the credit card vendor) to help make sure the card information hasn't been stolen
- Call the issuing bank and verify the customer's details

Credit Card Fraud Detection Services

Another step you can take to protect yourself against online fraud is to use a fraud detection service like MaxMind. MaxMind scores each transaction and alerts you when transactions look fraudulent. It does this by checking geographical locations, addresses, emails, Internet details and bank numbers. This information is also made available so you can make further checks by yourself. You have to pay for services like this, so there are different levels of protection offered to suit your risk levels and your pocket.

What to do if you've been defrauded

There are certain things you should do as soon as you confirm that fraud has taken place. Though it may prove impossible to recover lost goods or earnings, you can take action and hopefully prevent the reoccurrence of that particular fraud.

- Record all circumstances connected with the fraud – order details, customer information, dates, times, etc
- If the fraud involves a stolen credit card, contact the rightful card holder if possible and alert them to the theft
- Immediately contact the credit card processor or bank used in the fraudulent transaction
- If you believe you've received money from a transaction involving a stolen credit card, contact your own bank about how to refund the money to the cardholder
- Contact police or other relevant authorities to report the crime

Report online fraud in the US

http://www1.ifccfbi.gov/index.asp

Report online fraud in the UK

http://www.dcpcu.org.uk/

Report online fraud in New Zealand

http://www.police.govt.nz/

Conclusion

We may have painted a scary picture, but don't be put off ecommerce. Stores all over the world deal with the issue of fraud every day and are still successful. You can do the same - just make sure you stay educated and vigilant.

If you put appropriate preventive measures in place and have systems that check transactions for fraud, you can minimize the risk.

Appendix 1: common types of online fraud

Online intellectual property theft

You have intellectual property rights to any material you've created. This means you own exclusive rights to use, publish or sell that material. But when this material is in electronic form on the Internet, it could easily be copied and used without your permission. Text, images and multimedia you've created for your own website could turn up on someone else's site, for example. Or perhaps that software program you wrote gets illegally copied and distributed for free when you intended to sell it. Whenever your intellectual property is stolen via the Internet, you're a victim of online intellectual property theft.

Identity theft

It's easy to store and access personal information on the Internet. Unfortunately, that means it's also easy for people to obtain this information illegally. This is identity theft. Stolen details such as names, addresses, birth dates, and account or card numbers all build up an identity that can be used to commit fraud. Because online trading isn't face-to-face, it's easy for someone to hide behind a stolen identity and make fraudulent purchases or requests.

Phishing

Any email or website that requests private information such as credit card numbers, account numbers or passwords may be an attempt at 'phishing'. Any information you send to a phisher may be used unlawfully. Even if the request looks genuine, it is still sensible to make independent checks on its validity. For example, if you receive an email from a bank asking to confirm an account number, don't reply immediately. Ring your bank to confirm the request, and don't use any phone numbers included in the email – they could be fake.

Pagejacking

If you click on a link and find yourself at an unexpected website, you may have been 'pagejacked'. This happens when someone steals part of a real website and uses it in a fake site. If they use enough of the real site, Internet search engines can be tricked into listing the fake site and people will visit it accidentally. The fake site could contain unwanted or offensive material. As an online merchant trading via a website, you need to know that your site isn't being stolen in this way. Unfortunately you can't prevent pagejacking; you can only deal with it after you know it's a problem.

Advance fee scams

An advance fee scam is fairly easy to identify – you will be asked for money or goods upfront in return for giving you credit or money later. These advance fee scams can seem convincing and have taken in many people. One example of an advance fee scam plays out in online auctions. If a buyer sends you a check for much more than you asked, be suspicious. If you accept the check and refund the extra money to the buyer, you may find out later that the check was bad and that you've lost the whole amount.

Bad check scams

Always be wary of unusually large orders, even when the customer is paying in advance by wire transfer (an extremely safe method of payment when performed bank-to-bank). Though the transaction could be perfectly legitimate, pay attention if the customer asks for your bank's address or suddenly asks to pay by check instead of by transfer. In both cases, the customer may be about to pull a bad check scam. Both scenarios allow the customer to deposit money into your account by check. If the check is a clever fake and you accept it as payment, you lose both the money and the merchandise.

Fake money orders

Usually a money order is one of the safest ways to receive payment. The amount is prepaid by the customer, and a bank passes the amount on to the merchant. Because the money is handled via a third party and can be transferred internationally, many online transactions are made using money orders. They're difficult to counterfeit, but be especially cautious of money orders from high-risk areas such as Asia, Africa, Eastern Europe, the Middle East or Russia, as counterfeit money orders from these areas are unfortunately becoming more common.

Wire transfer fraud

As long as you avoid transfers via cash offices and stick to transfers performed bank-to-bank, wire transfer is a very safe way to move money around. This doesn't apply if you're asked to accept money and then pass it on to someone else via wire transfer. If that happens, be suspicious, especially if you're asked to do this by anyone you don't know well. You may think you are helping someone, but actually this is a form of money laundering used by organized crime. Though your money isn't being stolen, falling victim to wire transfer fraud can get you into trouble with the authorities.

Appendix 2: useful links

Credit card fraud

About credit card fraud
http://en.wikipedia.org/wiki/Credit_card_fraud

Protecting yourself
http://www.biz.org.nz/public/content.aspx?sectionid=75&contentid=399
http://www.antifraud.com/tips.htm
http://www.wiscocomputing.com/articles/ccfraud.htm
http://www.paypal.com/cgi-bin/webscr?cmd=_fraud-tips-sellers-outside
http://onlinebusiness.about.com/od/paymentprocessing/a/fraudsigns.htm
http://www.tamingthebeast.net/articles2/card-fraud-strategies.htm

Importance of credit card fraud protection
http://www.verisign.com/products-services/payment-processing/online-payment/fraud/why-fraud-protection.html

The Merchant 911 website
http://www.merchant911.org/

Credit card verification

The AVS verification system
http://www.tconsult.com/address_verification.aspx

The CVV2 verification system
http://www.visa.ca/en/personal/shop_cvv2.cfm

The SecureCode validation system
http://www.mastercardmerchant.com/securecode/

Phishing

Learn more about phishing and how to avoid it
http://www.mailfrontier.com/docs/field_guide.pdf
http://www.shef.ac.uk/cics/security/phishing.html

Pagejacking

Identifying pagejackers and dealing with them
http://www.tamingthebeast.net/articles4/pagejacking.htm

Advance fee fraud

http://www.secretservice.gov/alert419.shtml
http://www.tamingthebeast.net/articles5/nigerian-scams-ecommerce.htm

Intellectual property fraud

http://www.usdoj.gov/criminal/cybercrime/AshcroftRemarks042204.htm
http://eziniearticles.com/?Passwords-or-Pass-Phrase-Protecting-your-Intellectual-Property&id=7870

Online identity theft
http://www.tamingthebeast.net/articles/creditcardfraudidentitytheft.htm

Escrow (an alternative payment system for large international transactions)

About escrow
https://www.escrow.com/index.asp
http://www.a-e-a.org/

About escrow fraud
https://www.escrow.com/fic/index.asp

Postal money orders
http://www.usps.com/postalinspectors/moalert.htm

See the difference between fake and genuine
http://www.usps.com/postalinspectors/mofeatur.jpg

Online auction fraud
Lots of information about online auction fraud in this downloadable pdf file
http://www.ifccfbi.gov/strategy/AuctionFraudReport.pdf

Maxmind
http://www.maxmind.com/

General resources

Ecommerce fraud
http://www.knowledgeleader.com/iafreewebsite.nsf/2dcddc49dec9cd558525685400583e59/f36d97779d4e6e2288256cdf0070631b!OpenDocument

Internet fraud
http://en.wikipedia.org/wiki/Internet_fraud

More about different online frauds, including rigged auctions, investment scams, etc
http://pcworld.about.com/magazine/1905p107id44671.htm
http://www.canadiancontent.net/dir/Top/Society/Issues/Fraud/Internet/

Fraud information and reporting in the US
http://www.fraud.org/

High risk countries of 2004
http://www.msnbc.msn.com/id/4648378/