



International Ecommerce Do's And Don'ts

**Keeping Your International Ecommerce
Wealth Safe From Fraudsters**

[Coble International](#)

Keeping Your International Ecommerce Wealth Safe From Fraudsters

This report is being published with the emphasis being on a USA based business – if you happen to be based in another country, simply apply what is being provided to your own country to gain maximum benefit.

International ecommerce and doing business globally often conjures up dreams of incredible wealth for many people. While extremely lucrative global profits can be earned online, this report is being written to provide you with guidance, from real life experience, on how to protect those profits from being lost to the worldwide epidemic of fraud that the Internet has also unleashed.

Conducting international business using ecommerce can involve B2C (your business selling to individual consumers) or B2B (your business selling to another business). Considering the population of worldwide Internet users as being over 6.7 billion people, which only represents a 23.8% penetration; one can easily see why you could dream of incredible wealth.

TIP: For information about international B2B and B2C ecommerce, read the report: International Ecommerce Do's And Don'ts; B2B or B2C? (a short companion report to the 'Keeping International Ecommerce Wealth Safe From Fraudsters' ebook)

With all good things, comes some that are not so good and although this report may seem heavily focused on the “bad”, it will hopefully help you see the both rewards, risks and help you determine if you, your product and your business are ready for “international prime-time”.

There are many service providers who will contact you after your web site is found by the search engines and they will argue, sometimes very convincingly, that you need to get your site represented in the international markets.

Some will be selling translations services where they will charge you hefty fees to translate your pages into various languages that they feel are worth entering. Others will try to sell you on getting your web site listed in various foreign search engines.

Quite frankly, if your web site is less than 4 or 5 years old, you probably have not penetrated even a small portion of your domestic target market, let alone the English speaking audience.

TIP: ENGLISH IS THE LANGUAGE OF INTERNATIONAL BUSINESS!

Most countries teach English as a second language and our little international ecommerce website has sold products into 68 countries and your author can only speak a few words of Spanish (none of which have been helpful in my 21 years in this business).

The focus of your ecommerce website should be, first and foremost, focused towards visitors who speak your native language. If that language is something other than English, then focus on your

home country and consider developing an English translated site, “when” and if your native language sales warrant this expansion.

In regards to getting your web site ranked in foreign search engines, here again, focus your attentions and time on getting your site ranked in the major search engines of your home country first. The more you focus on getting your site listed in Google, Yahoo and MSN, your site will have a better chance of being picked up on foreign search engines through natural osmosis.

Many, if not most, foreign search engines do not allow submissions of web sites from outside the country in which they are based, thus most of any money or time you spend trying to get listed in these engines will be wasted. Focus on your native country search engines and let the rest to natural assimilation.

TIP: Be sure to quote your price in US Dollars so there is NO misunderstanding when the person’s credit card is charged in their currency!

If you ship anything internationally or domestically, without some form of tracking, you stand a good chance of getting the item charged back against your merchant account. Too high a charge back percentage not only costs you in charge back fees but could end up costing your business its merchant account.

TIP: For essential information about shipping and customs, read the report: International Ecommerce Do's And Don'ts; International Product Shipping Methods And Custom Forms (a short companion report to the 'Keeping International Ecommerce Wealth Safe From Fraudsters' ebook)

The Good, The Bad, And The Fraudsters

As I said in the beginning, this report is not meant to dissuade anyone from joining the forces for good in International Ecommerce. However, as I also stated, with the good, you must also be prepared for the bad and ultimate for the lowest of low-lives, the FRAUDSTERS.

The GOOD aspects of international commerce are too numerous to mention. A few include new markets, increased profitability, etc.. The fact our small B2B business (and some B2C) has sold products and services in at least 68 countries provides solid proof of how lucrative it can be.

On average, about 40-45% of our business comes from sales originating from outside the USA and we have experienced years where it has been upwards of almost 70%.

Our international ecommerce web site has been responsible for allowing me to take an early retirement from a JOB about 6 ½ years ago which is something that simply would not have happened had we not been doing so much business internationally.

The BAD aspects involve the extra amount of shipping documents you have to prepare, the difficulty in verifying credit card information with banks outside of North America, the difficulty

in communicating with people who know how to speak English but who speak it very poorly and some of whom do not understand your correspondence, either verbal or written.

The above represent what I would call the Easy Bad aspects because ultimately, with persistence, and patience, most can be overcome and a transaction can be completed.

The Fraudsters

Fraudsters can be “the bane of your life” (not sure what bane means – go look it up).

This is a subject near and dear to my heart because if I can prevent ONE person from being ripped off by the fraudsters, I will have accomplished the biggest goal for writing this report. I speak as someone who has experienced well over ½ million in fraudulent orders in the last 8 years – yes, that is over \$500,000 in 8 years.

It does not take long to accumulate that type of value when you sell databases that go for \$1,955 or as the biggest single one received yet (just in May of 2009), \$3,995.00 for one single database.

Thankfully, other than a few charge backs amounting to a couple of hundred dollars, we have not been burnt by any of the outright FRAUDSTERS who have been drawn to our web site like moths to a flame.

We encourage people to visit our web site “About Us” or “Company” page as a means of checking us out before they do business with us. They are also encouraged to use a group of “DUE DILIGENCE” resources we have posted on that page to help them in checking us out but more than that, use these resources to check anybody and any business they are considering doing business with.

Visit our company page, scroll down to where you will find the DUE DILIGENCE resources and be sure to bookmark that page so you may use it as a reference for future transactions - <http://www.importexporthelp.com/company.htm> - I use those same resources (and more sometimes) on a daily basis.

Every order that we receive, whether domestic to the USA or international, receives a variety of checks against it and the names, emails, phone numbers, credit cards on it.

The fraudsters will often use PROXY servers to place an order which makes it appear the order originated in the USA but it actually was placed from one of their internet café's in Nigeria, Benin, Ghana, and Indonesia (those are some of the top fraud originating countries).

Tip: Install IP Tracking On Your Ordering Or Shop Cart System

IP tracking is not failsafe, as mentioned above. Proxy servers are used to trick your cart into showing it originated from another location.

However, at one point, we were receiving 10 fraud orders for every 1 legitimate. The frustration of dealing with all this was getting out of hand. A javascript IP tracking code was installed on our ordering system so the fraudster could see their IP and could not change it (it was read only).

This visible tracking reduced the overall ratio to about 4 to 1 which is bad but more tolerable. It did increase the number of proxy fraud orders but still the ratio is less than half of what it was before. Once the light of day is focused upon these scum of the Earth, they tend to crawl back under the rock from whence they came.

My preferred web site to check the location of an IP is: <http://whois.domaintools.com>

Fraudsters Are Like Bacteria – They Adapt

As I mentioned earlier, our international trade marketing services business attracts fraudulent orders like moths to a light on a summer night.

The primary reason for these orders has been the directories we offer that contain the contact information for one hundred and fifty thousand worldwide importers. Always expanding our B2B services, we now also offer databases totaling over 19 million listings from businesses in the USA, Canada and Mexico.

The fraudsters attempt to use one form of fraud (stolen credit cards) to purchase our directories which they will then use to email, fax or mail their infamous "Nigerian" scam proposals.

These proposals are no longer limited to being just from Nigeria and the methods of their madness in attempting to extract funds from the poor soul who is foolish enough to not perform even the minimum of due diligence.

Our "fraudster flood" really kicked off in 2001 and has now totaled (as of May 2009) well over \$500,000 (I save the orders to prove this figure should anyone wish to challenge me). Thankfully, however, because my methods of due diligence are utilized for both foreign and domestic orders, we have not lost a cent to a fraudulent order.

But, the war being waged by the fraudsters is getting (or has gotten) even more difficult because fraudsters are like bacteria, they adapt.

A few years ago I had an order from South Africa (hereafter referred to as SA). It was for two Mexico Business directories with a total cost of \$1,390.00.

The order upon initial review, looked fairly legit, spelling was good (misspellings are a definite flag), the first and last names were not reversed (for whatever reason, they often put the stolen credit card owner's last name in the first name area and first name in the last name area – this is an easy way to spot new, not to educated fraudsters).

The email used with this SA order was a free email (another definite security flag) but the IP address on the order checked out as being in South Africa - things were looking "fairly" positive.

The next check was the first 6 digits of the credit card with our merchant services bank lookup which is a great service that if your merchant account does not provide, you should lobby them to do so since it benefits them as well as you.

The next BIG security flag was raised with the bank lookup because the credit card issuing bank was located in Mumbai, India.

This was enough to cause me to request the customer submit a faxed or scanned copy of the front and back of their credit card via fax or scanned attachment to an email and the "TOP" portion of a recent billing statement so we can verify the billing address he had submitted (we emphasize the top portion because we don't need to see their transactions - just their address).

The next morning, I had a two page fax waiting for me. The first page went into great detail to assure me that because he is currently on travel and therefore he did not have a billing statement to submit but he assured me that he was indeed the owner of the card.

Now what was interesting about the copy of the credit card was that it had the number, expiration and name imprinted on it but you could not see any bank info, logo or other details?

On the back side the number in the signature area and the CVV number matched but the card was not signed and again, none of the other info you normally see on the back of a card was there, nothing??

The icing on the cake came when I got a call from this individual shortly after reviewing the fax. He was asking how quickly he would get his order, whether there was a download link where he could get it rather than waiting for a CD to arrive.

When they are extremely anxious to get the order shipped right away and are willing to pay whatever price necessary to ship it, this absolutely is a HUGE FLAG because quite literally they are not paying to get it shipped, the credit card owner is, but bottom line, you are because the credit card owner is protected, you as a vendor, are not.

Enough flags, I called the issuing bank in India and unlike most card issuing banks in English speaking countries (UK and Australia – sorry, just relaying experiences) the security department in the Mumbai bank was very helpful and advised that the card's billing address was in India, not South Africa.

Shortly after posting the above experience in a business forum where I am a member, someone who worked with credit card companies posted that indeed the bacteria (fraudsters) had adapted.

It seems the fraudsters now had the plastic credit card blanks and imprinting machines so they could imprint the numbers onto a blank and take one more step towards making their orders look legit.

This was 3-4 years ago, I have not had another one like it since, however, it would not surprise me if they have found a method of imprinting logos and such to make the cards look even more legitimate.

Tip: If a foreign customer calls or emails expressing their extreme need for whatever it is they are buying – BE CAUTIOUS, BE VERY CAUTIOUS

Generally, the reason for the extreme SPEED they ask you to deliver an ordered item or service is because the credit card has not been flagged yet as being stolen.

If you process after finding the type of flags described above and ship or deliver the goods or services, it will most likely end up costing you many ways, including:

- A charge back fee which the last time I checked was about \$35.00 for 'each' one
- The loss of the value of the item or service you shipped or provided
- The shipping costs
- And potentially your merchant account if you process too many fraud orders that end up raising your charge back rate to whatever level your merchant provider deems too high

International Payment Alternatives

Western Union or American Express money transfers are safe alternatives for you, as a vendor, however, they then place the burden of due diligence upon the foreign customer and unless you have a long Internet verifiable history, these options will turn many potential customers away.

Next up are Bank Wire Transfers.

Bank wire transfers are still another option that places the due diligence responsibility upon the customer and they are difficult to obtain in some countries.

Our business has received payment through all 3 of the options mentioned above but there are some drawbacks to the bank wire transfers that will be covered next.

Tip: If you have electronic banking that allows direct deposit into your account for wire transfers, pay checks, etc. by authorizing direct electronic deposit YOU HAVE ALSO AUTHORIZED 'DIRECT ELECTRONIC WITHDRAWAL'

Some bank employees will actually deny this, basically because they are ill-informed or never informed of it, however I learned this lesson about 15 years ago when the company my wife worked for decided to use direct deposit as their sole method of paying their employees.

When I reviewed the next statement from the bank (we did not have Internet banking in those ancient days) it indicated that her employer had deposited the amount of her check 3 times. All was well with that ;-), but then they subsequently withdrew the same amount '3' times, then ultimately deposited the right amount one more time.

I contacted the bank about why the company was allowed to take money "out" of the account, they stated the following: "when you authorize a company or anyone to deposit funds into your account electronically, you are also authorizing electronic withdrawal of funds from that account".

OK! This was something new that very few people knew about then or know about today and which can be very important to you, if you intend to use Bank Wire Transfers as a method of receiving payments..

Why?

The potential payer of the bank wire transfer will need your bank's ABA/Swift numbers along with your account number in order to send you the money.

If you provide your bank account information to a prospect in good faith for them to use in sending you funds to purchase your goods or services and the account information you provide is for the only business account you have, **you are exposing all of those funds to potential loss.**

I know because I speak from EXPERIENCE!

In our first bank account fraud incident, there was approximately \$350 in the account we maintained for specifically for bank wire transfers. The \$350 had been received from a customer who had purchased one of our trade directories, plus the small balance we maintained in that account.

A fraudster who had requested our bank account info under the pretense of purchasing a trade directory hit our account with four \$500 electronic withdrawals for a total of \$2,000.00.

The electronic banking system, as it is, transferred those four \$500 amounts from our account even though there was only approximately \$350 in the account.

The bank then proceeded to charge us 4 separate insufficient funds charges and added insult to our injury by charging us 4 transfer fees all of which amounted to about \$240.00.

Because we were monitoring this account in anticipation of the transfer we were expecting, we caught the fraudulent withdrawals within 24 hours of their posting. We immediately notified the bank and the account was frozen and provided the bank with written authority to investigate the fraudulent withdrawals.

The bank employees informed me that this happens to them several times a day and were very helpful and they refunded all fees and replenished the account to its original balance before the fraudulent withdrawals. Had we not caught this as quickly as we did, the story may have been different.

The waste of your time factor still comes into play here because the account had to be closed, a new one opened this is time lost for both our business and the bank.

A few of my business associates who I have told this story to inquired at their bank and were told that this would not happen. It does, it will and yes, it can happen to you – I have reason to tell you this other than to inform you about what can and will happen to you if you do not follow some of the precautions that will be outlined a little later.

Shortly after this incident, the Maryland state banking commissioner was interviewed by a Baltimore TV station about this very thing happening on an ever increasing basis. The reason for

this broadcast segment was due to a domestic business that was using electronic withdrawals from people's account without their knowledge that they had inadvertently authorized those withdrawals.

The Maryland state banking commissioner was asked about this type of fraud. He reluctantly admitted that there was little anyone could do to prevent these unauthorized withdrawals because once you authorize automatic electronic deposits, you are also authorizing electronic withdrawals.

The second fraudulent withdrawal incident occurred just a few weeks ago during the last week of April 2006.

Another fraudster, who corresponded with me for nearly almost two weeks "by email" regarding the purchase of a trade directory and ultimately decided he wanted to pay via a bank wire transfer. I found this "somewhat" suspicious from the start since the address they gave us for delivery was from here in the USA.

As the correspondence continued more information led me to believe this was a legitimate request (but I was still a bit suspicious) so I provided our wire transfer account information but began checking the account several times a day rather than once a day.

In the pro forma information I provided this fraudster, I advised him that we maintain a balance of less than \$25.00 in this account for security reasons and to prevent unauthorized withdrawals. Stating this was in the hope that \$25.00 would not be worth their time and effort.

I did not hear from him again until I saw the pending withdrawal from our account about two weeks later for \$24.75. **Can you believe it - \$24.75?**

I immediately notified the bank but it was a Friday evening so nothing could be done to prevent it.

However, there was a web site listed in the pending withdrawal information. I looked it up and found that it was an online financial transaction firm for porno web sites.

Apparently this guy figured that \$25 is enough to pay for his entertainment for whatever amount of time it would buy him.

However, it did not buy him much because the online financial firm had a phone number, I called and told them what happened and that the transfer from my account was fraudulent. They immediately shut down his account and set up a return of our funds.

Good news 'again', the funds have been returned, but this incident has again caused us and the bank much time and effort and again even more wasted time.

To prevent any further unauthorized withdrawals, I had to place a permanent freeze on the account for electronic withdrawals.

I was still able to use this account to receive my bank wire transfers but I can no longer use my Internet access to transfer that money to another business account which is what we normally would do to prevent the funds in the transfer account from being exposed to this type of fraudulent activity.

Now, we have experienced multiple incidents, I must physically, visit the bank, produce my driver's license and ask them to move the funds out of the wire transfer account into our other business account.

Fraud costs everyone involved time and money. In this incident I hope it also caused the fraudster the loss of his anticipated entertainment.

TIPS: Some Points To Help Keep Your Business From Being A Fraud Victim

- 1.** Set up a separate account just for wire transfers – most banks have low balance, no fee, no interest checking. Set one of these accounts just for your wire transfers.
- 2.** Keep a balance of \$25-\$35 in this account or just enough to pay the fees for an incoming wire transfer.
- 3.** Get Internet banking so you can monitor for receipt of the transfers - as soon as you see the funds are available, transfer them to your main business account.

This does not prevent a fraudster from doing as they did with us and hitting the account with multiple withdrawals but it gives the bank more incentive to help you resolve the situation if it is 'their' money they give out rather than yours.

- 4.** Make sure you require 'complete' information from your would-be customer - do not give out your bank information to just anyone who asks for it.

Again, this is not 100% fraud proof as I had this latest fraudster fill out our Pro Forma request form before I provided him with our information, however, by asking for all of their contact details like we do on our pro forma request form, it makes most fraudsters crawl back under the rock from where they came.

- 5.** Be very careful (sorry if I offend anyone here but it needs to be said) of anyone who uses a free email account like yahoo, hotmail, gmail or a host of others that are out there. I have multiple gmail accounts myself, but they are fast becoming as bad as yahoo and hotmail when it comes to fraudulent use.

If you are not sure of a particular email account, you can find out if it is a free email provider by taking their email address and typing in the domain.com, .net, .org, .us, etc. into your browser window to see if it is a freebie account.

Again, there is no guarantee that a real web site that shows up today will be around a month or a year from now. There are services that allow you to have a one page web site with full email privileges for under \$20.00 a year.

As President Reagan used to say, "trust but verify", but when it comes to international ecommerce transactions or other business transactions involving bank wire transfers, I say "verify, verify, and verify some more".

TIP: Sign Up For The FBI's FREE New E-Scams & Warnings At <http://www.fbi.gov/cyberinvest/escams.htm> - DO IT TODAY!

Much of the following information has been provided by the FBI (the numbered paragraphs) but I added my personal **Cautions and Beware Of's** at the end of each of their recommendations.

Let me begin by **CAUTIONING** you - Cashier's Checks or Bank Drafts can and are often fakes - do not believe for one minute that just because they tell you it is a Cashier's check or bank draft that it is safe to ship your item or import export merchandise.

If you can answer "YES" to any of the following questions, you could be involved in a FRAUD or you are about to be SCAMMED!

1. Is the CHECK you received for an item you sold on the Internet, such as a car, boat or jewelry, etc?

Ron Coble Note: (RC Note) Checks can take up to 21 days or more to clear USA based banks and up to 30 days or more if drawn on a foreign bank. With full color printers it is very easy to fake a check to appear like it is legitimate and it could take 30, 60 or even 90 days for a check to bounce back from a foreign bank. Do NOT ship any merchandise until you know funds are secure and I personally "would not" accept a check from out of the country as payment for anything.

2. Is the amount of the CHECK more than the item's selling price?

RC Note: This is a very common scam but not one that many people are aware of. The scammers prey upon the kindness of people to help 'them' get more US cash back into their country by using this method by telling them how difficult it is to do this otherwise. They are also always willing to pay you the full asking price for the item you are selling with no negotiation - clear sign this is a fraud/scam.

3. Did you receive the CHECK via an overnight delivery service?

RC Note: This is a method to try and close the scam/fraud as quickly as possible and to also impress you on how they are true business persons by using overnight delivery.

4. Is the CHECK connected to your communications with someone by email?

RC Note: Remember on the Internet that anyone can pretend to be anyone and thousands of web sites offer free email accounts. Always beware of someone who is using a free email account as their sole email communications when it comes to any import export business or personal financial transaction.

5. Is the CHECK drawn on a business or individual account that is different from the person buying your item or import export products?

RC Note: The buyer could be using stolen checking account information and the other part of the scam sometimes involves an actual person residing in the USA who delivers the check making the scam look even more legitimate.

6. Have you been informed that you were a winner of a LOTTERY, such as Canadian, Australia, El Gordo, or El Mundo, that you did not enter?

RC Note: Use a little common sense here my friends, it's time to wake up from watching too many (un)reality shows and dreaming of a generous millionaire/billionaire coming to your door with a check.

7. Have you been instructed to either 'WIRE', 'SEND' OR 'SHIP' MONEY, as soon as possible, to a large U.S. city or to another country, such as Canada, England, or Nigeria?

RC Note: This refers back to my note above about the scamsters having accomplices living here in the USA. I am going to repeat myself here many time, please forgive me, but please USE YOUR COMMON SENSE and UNDERSTAND that IF IT SOUNDS TOO GOOD TO BE TRUE - IT IS!

8. Have you been asked to PAY money to receive a deposit from another country such as Canada, England, or Nigeria?

RC Note: This scam has been going on for almost all of the 18 years I have been in the import export business, yet each year I read about some trusting soul who did not USE THEIR COMMON SENSE who falls for this scam.

They used to do this by registered letters. I don't know how many wasted trips I made to the Post Office to sign for a registered letter that was from one of these scamsters. Many of them could be accomplished authors if they tried since they write these compelling stories about their husband, father, uncle etc. who was part of their countries government and how he was brutally killed and now their relatives need "you" to help them get the money out of their country.

There are 1000 different stories, they used to only come from Nigeria, then they began coming from all areas of the world. They went from registered letters to sending fax messages and then the goldmine of fraud came along - Email - free easy, they can now blanket the world with their net and it costs them nothing to lure in some poor unsuspecting person who simply got overwhelmed with the prospect of instant, no hard work wealth. Please, don't let it happen to you.

9. Are you receiving or being offered to receive PAY or COMMISSION for facilitating money transfers through your account?

RC Note: First, giving out your account information to 'anyone' is very, very dangerous. Once a person has your bank account information to 'supposedly' put money into your account, guess what, they can take money OUT of your account.

10. Did you respond to an email requesting you to CONFIRM, UPDATE OR PROVIDE your account information?

RC Note: Even I, after all my advice to everyone else, fell for one of these fake emails supposedly about our Ebay account. It caught me off my usual guard. It was early one morning, I was not quite awake yet and the email appeared to be legitimate, had eBay's logo, everything appeared normal. I clicked on the link and logged in. Luckily I had that gut wrenching and sinking feeling immediately upon doing so that I had just been had.

I immediately went to eBay's site by typing it into my browser window and logged in and changed our password to a 15 letter/digit one and prevented any further problems.

I did learn later however, that by clicking on the link in that email, I may have planted a spyware program on my computer which could record every keyboard click (including my passwords, userids, account numbers, etc.) and send that info back to the scamster who planted it there. Using a free spyware recommended by Cnet's Download web site, I cleaned up my computer from any possibility of this. Here is a link to Cnet's site you can copy and paste into your browser window:
http://www.download.com/Spybot-Search-Destroy/3000-8022_4-10122137.html

Closing Remarks And Recommendations About Fraud Prevention

Much of what you will read on the Internet is written by paid writers, who in most instances have little or no actual experience or life experience with their subject matter. They write based on research they do into the subject and usually their writing is lacking in real life experience.

When it comes to Fraud and Scams, the comments and recommendation provided in this report are from my personal experiences and only represent a SMALL fraction of those experiences.

Many very highly educated people can fall prey to fraudsters – here is a link to a post I did in an older newsletter several years ago – check it out and learn how a Dentist was defrauded out of a large sum of money and how -
<http://www.importexporthelp.com/b2b/world-business-exchange-14.htm>

In concluding, as I mentioned earlier, this report was not written to dissuade you from joining in the profits that can be made with International Ecommerce. Instead, the report is designed and written to help prevent you from being a victim and losing out on the profits that are legitimately available to you and your business.

Hopefully, what has been revealed in this report will also help you determine if selling your products and/or services will be worth the time and effort required to sell them into the international marketplace.

The B2B market is much better suited to international ecommerce, in my humble opinion, than the B2C market. Some of the due diligence recommendations referred to in this report, simply would make a small transaction too time consuming to be worthwhile.

I hope this report will help you make a more informed decision about International Ecommerce in regards to your business and that you have found my experiences both interesting and worth reading.

Ron Coble
Coble International
<http://www.importexporthelp.com/>