

eMarket Services makes it easier for you to use  
electronic marketplaces for international business

## **EMARKETPLACES AND THE ISSUE OF FRAUD – AWARENESS THROUGH EDUCATION**

**Peter Saint**

eMarket Services

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

December 2009

# Report



## Abstract

This is the second report, in a three-part series, aimed primarily at SMEs who would like to increase their awareness, and educate themselves in relation to eMarketplaces.

As eMarketplaces (B2Bs) continue to grow and bring continued economic benefit to small and medium-sized enterprises (SMEs) via their online strategies for international growth, it is imperative that the SME comprehends the issue of online fraud.

As a previous B2B website owner, from experience I understand the necessity of SMEs educating themselves on the issue. It is only through education, and awareness, that an SME will be able to recognize the techniques employed by individuals attempting online fraud, therefore, empowering the SME to only transact in genuine and profitable business transactions.

*Keywords: Fraudsters, Online Fraud, Fraud Techniques, Internet Fraud,*

## The Author

Peter Saint has spent 10 years involved with eMarketplaces creating Eurecycle.com and then working as CEO of Globalrecycle.net.

Currently, he continues to work in an advisory capacity for emarketservices.com as well as operate his own e-consultancy business. If readers wish to comment, question or highlight any issues raised by this report, Peter can be contacted at [peter.saint@emarketservices.com](mailto:peter.saint@emarketservices.com)

## Online Fraud and Online Fear

Online fraud is the fear of many SMEs particularly when mainstream media focuses intently on stories with negative headlines in relation to companies, or individuals, being defrauded on an almost daily basis. However, when you contrast that fear against figures as recently reported by China's Ministry of Commerce; stating that e-commerce transaction volume for 2008 were estimated at RMB 3.1 trillion (USD \$453m) for China alone (<http://www.hktdc.com/info/vp/a/dml/en/1/3/1/1X05RPHG/Design--Marketing---Licensing/China-s-e-commerce-transactions-hit-RMB-3-1-trln-in-2008.htm>) then these fears have to be displaced by knowledge and awareness of when, and how, to recognize the issue of attempted fraud. By making your SME aware of the issue, and educating yourself on the topic, your company will, I believe, be able to discover potentially very lucrative new international markets via eMarketplaces and online fears of fraud will dissipate.

*eMarket Services makes it easier for you to use electronic marketplaces for international business*

## Techniques Adopted by Online Fraudsters

As well as being aware of verifying whether a company registered on an eMarketplace is genuine or not, it is equally important to be aware of the techniques that fraudsters use in order to scam genuine businesses. By educating yourself and being aware of the issue of online fraud, you will increase the likelihood that you will be able to only participate in genuine and successful national and international business. From my experience, online fraud is usually successfully perpetrated against those who are not aware of the issue, and, in particular, are blinded by the idea of making vast sums of money online quickly and very easily.

My role in the promotion of international trade using a B2B e-commerce website has assisted in expanding and growing SMEs by opening up new international markets. However, when your SME views that first, potential business opportunity the adage still applies in online, as well as offline, business: "if it sounds too good true then it probably is." That would be my first, and most important, rule of online fraud awareness.

Below we'll explore a couple of prominent techniques fraudsters adopt – the list is clearly not conclusive as techniques through time, adapt and change – the importance is raising your awareness of the issue and how to recognize it.

### 1. Deposits

Through my ten years of experience the most common, and the simplest, attempt at fraud via an eMarketplace is to fraudulently deceive a company out of a security deposit. There are various techniques to this, but in essence it works like this: a seller (fraudster) contacts the genuine buyer, via an eMarketplace, to make an offer on goods/services they are looking to buy. The buyer expresses an interest and, after negotiation, is asked to send a 10-20% security deposit to secure the deal on the non-existent items/service. Once the deposit is sent the buyer never hears from the seller again and the deposit is gone. Depending on the nature of the business, deposits can be highly valuable. Therefore, before sending a deposit you have to be very confident that the company you are dealing with is genuine. Transfer payment companies, such as Western Union, have explicit warnings against sending money to individuals/companies that you do not know:

<http://www.westernunion.com/info/fraudIndex.asp?country=global>

If there is any doubt, or you do not have enough information to verify the prospective business partner's authenticity then exercise caution until the doubt has been lifted.

Further to this be aware of the longer-con which involves two small transactions concluding without any problem and then the seller offers a high-value transaction which is not only very profitable to the buyer, but involves a much larger security deposit. As an element of trust has been built between the two companies the buyer feels assured to send the larger deposit. However, when the large deposit is sent the seller disappears. It is imperative that if there is a sudden dramatic increase in a transaction's value in relation to earlier transactions that you use alternative methods to verify the authenticity of the deal. For example, factor-in the travel cost; go view the seller's premises and their proposed goods/services.

## **2. Shipping Low Quality or Worthless Goods**

A transaction has been concluded via an eMarketplace and the buyer has had an opportunity to not only view the quality of the material via online photographs, but a sample has been sent which has been verified. Payment has been sent and the seller has sent photos of the containers being loaded and shipped to the buyer. When the material arrives at the buyer's warehouse, or port of entry, it is discovered that the material sent was not what was agreed upon, but is in fact worthless. The supplier has either disappeared or refuses to take the material back. When concluding business for the first time it is advisable to consider using an escrow service. Although fees will have to be paid to the escrow service, it will help stop the potential for low quality goods being sent – if low quality goods are sent whilst using escrow they can be returned and your payment will be returned to you. Some eMarketplaces have direct links with escrow services.

## **3. The Large Contract**

SMEs are always willing to land that large, long-term contract which will generate increased revenues and profits for their business for the foreseeable future: understandably, securing their long-term future. Fraudsters, unfortunately, are also aware of this fact. One fraudulent technique used by fraudsters is as follows. A buyer places an advert on a B2B website, and they receive a response from a seller offering a large contract. However, the seller is inviting the buyer to come to their country, so that they can meet and conclude the transaction. Due to the size of the contract it appears feasible for the buyer to travel to that country, also, by meeting with a new potential business partner helps build trust. So the buyers agree to travel. The seller will suggest an expensive hotel to stay at and arrange a time to meet. At this point several potential scenarios will occur, of which I'll highlight a couple, but the end the result is the same – attempts to try and defraud the buyer.

After meeting, the seller suggests that before proceeding to business that both buyer and seller visit a shopping mall, and once there enforce upon the buyer that it would be positive for business relations to buy an expensive gift (normally in the thousands of dollars) for their VP or President's Wife, for example. Once the buyer purchases the "gift" and presents it to the seller, he or she will find that the seller will very quickly disappears. Similarly, the seller may agree to meet at the buyer's expensive hotel and suggest that as the contract they are bringing is so large that the buyer should spend a few thousand dollars upon the seller within the hotel as a form of business goodwill. At all times during the lavish spending the sellers will avoid talk of business, and inform the buyer that they will return the following morning to sign the contract. However, they will not appear. As I explained earlier, there are many variations on this technique, but the principal is the same. A seller convinces a buyer that their company is about to sign a highly lucrative contract; the buyer has to travel to the seller's country to sign the contract; the seller convinces the buyer to lavishly spend money (normally in the thousands of dollars) as a goodwill gesture; the seller disappears. The buyer has spent on airfares, accommodation, additional expenses and been defrauded out of several thousands of dollars.

## In conclusion

As explained earlier, awareness and education are part of the ongoing battle against online fraud. Currently, no eMarketplace can verify all of their users' authenticity, so your own due diligence is paramount. Many companies use eMarketplaces successfully, and you can too, but never rush into a transaction with a new, prospective business partner, and remember, if a potential deal sounds far too good to be true then it probably is. By keeping those points in mind; you will discover that you can open new national and international markets for your company, allowing it to grow successfully, and in an atmosphere of trust, whilst using eMarketplaces. The final report in the series will look at practical experiences and testimonials of SMEs in relation to the issue of fraud and verification techniques.