

Fraudulent auctions on the Internet

Bezalel Gavish · Christopher L. Tucci

© Springer Science + Business Media, LLC 2006

Abstract Trust is an important ingredient for fostering the development of electronic commerce on the Internet. Recent statistics report on the growth of fraudulent activities on the Internet. We report the results of an investigation that checked for the amount of fraudulent activities on auction sites. The results indicate a significant level of fraudulent activities, well above the levels reported by auction site operators. Since fraud can be a major stumbling block for increasing the volume of electronic commerce on the web, it motivated further research on trust building activities given the prevalence of fraudulent activities on the Internet. We describe methods used by swindlers in their online swindling activities and propose methods to reduce the impact of fraudulent activities.

1. Introduction

Fraud is becoming a major hindrance to the development and use of commercial activities on the Internet. The *Financial Times* reports that online fraud represents “an epidemic of huge and rapidly growing proportions” and that the incidence of fraud is 20 times higher in online trades than in offline trades (Waters [12]). VISA claims that half its credit card fraud complaints come from Internet-based transactions, this in spite of the fact that only 2 percent of its transactions originated on the Internet (BBC [1]). According to a VeriSign study [11] 6.25% of e-commerce transactions carried out in the U.S. were attempts at fraud. More than half the fraud attempts were made by entities outside the U.S. Also, the number of security fraud incidents almost doubled between May 2003 and August 2003. One area that is of particular interest is the one of fraud in Internet-based auctions. The number of cases of auction fraud reported to the Federal Trade Commission in the USA has jumped from 106

B. Gavish
Southern Methodist University
e-mail: gavishb2000@yahoo.com

C. L. Tucci
École Polytechnique Fédérale de Lausanne (EPFL)
e-mail: christopher.tucci@epfl.ch

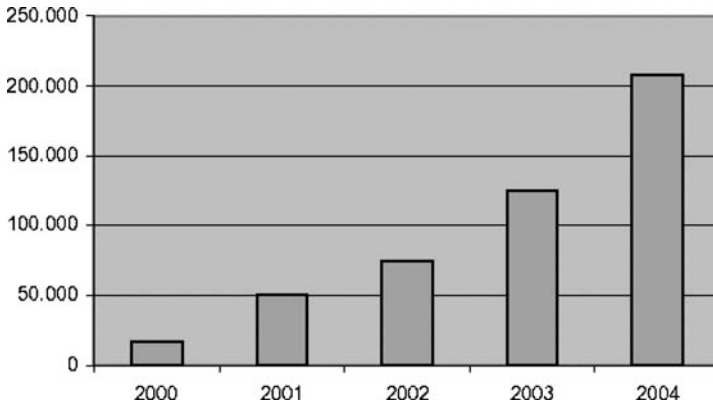


Fig. 1 Number of yearly complaints received via IC3 Website (2000–2004)

in 1997 to around 25,000 in 2001 (Reuters, [8]). At the same time major Internet auction sites estimate that fraudulent outcomes occur only once in approximately 10,000 auctions, which seems at odds with the above trends and statistics. The number of Internet-based fraud complaints is increasing at an alarming rate. Figure 1 displays the yearly number of fraud complaints received over the last five years.

In terms of monetary loss in the year 2004, 52.7% of the complaints were in the range of \$100–1000, with close to one percent of the complaints having a monetary loss in the range of \$10,000 to over one million dollars per incident. Many fraud cases are situations in which the defrauded person/s considers the amount in question to be too low to warrant spending his time reporting and/or going after the swindler, or cases in which the defrauded person is protected by insurance. In such cases, he does not have the incentive to report the swindling activity. Financial institutions and institutions whose business activity rely heavily on the customers having a perception that they are trustworthy institutions have the incentive to keep information on swindling activity in house,¹ maintaining an external image that they are safe and secure. Thus, we can safely assume that only a subset of the fraudulent activities is reported and the magnitude of the real problem is much larger.

Having a high degree of fraudulent activities on the Internet has a negative effect on the level of electronic commerce activities on the network. If consumers have the perception that conducting commerce on the Internet is not safe, it will have a damping effect on their willingness to conduct such activities. Thus, it is important to understand what methods are used by swindlers in their swindling activities, discover the frequency of cases in which they use the different methods and develop methods that reduce the likelihood that using a method will be successful. In the next section we present and discuss the different methods used for trust creation in the physical world.

Section 3 presents some of the methods used by swindlers in their swindling activities, section 4 presents results of a study of swindling activity on an online auction site, followed by conclusions and recommendations.

¹ This can be verified by observing the level of reporting before and after California passed legislation requiring reporting identity theft incidents.

2. Trust and trust creation

Trust can be defined in many ways, one of which is due to Kollock [6] “An action demonstrates trust if it increases one’s vulnerability . . . to another whose behaviour is not under one’s control”; in this definition, one party relies on the responsible behaviour of the second party. Trust and trust formation have received extensive treatment in the social sciences literature. Recently, due to its importance in economic activity, it has attracted research by economists; for example, Knack and Keefer [5] demonstrate an increase in national economic growth due to a rise in the level of trust. Alan Greenspan in his (1999) report to Congress said “Trust is at the root of any economic system based on mutual exchange . . . if a significant number of people violated the trust upon which our interactions are based, our economy would be swamped into immobility”. Political scientists have also investigated the relationship between trust in society and the efficiency of governmental institutions (e.g., Putnam [7]).

Trust is recognized as an important factor in facilitating further development of electronic commerce on the Internet. Widespread electronic trades and exchanges can take place if the traders can explicitly or implicitly (through the trade mechanisms) trust each other and the procedures used to conduct the electronic trade. A significant number of investigators have addressed trust issues; however, due to its complex nature the formation and management of trust in web-based environments raises many new research issues. One of the main concerns in trading on the Internet is the virtual interaction between entities whose physical attributes are not known and can be misrepresented. By its anonymous nature, virtual interaction is a fertile ground for fraudulent activities [2,3].

Before analyzing trust in an electronic virtual environment, it is important to understand the processes and mechanisms through which trust is created in the physical. They can include trust between individuals, trust between corporate entities, and trust between tribes or nations. Trust building mechanisms have to consider national versus international trust. We concentrate first on trust creation and handling between individuals. Trust is of concern whenever at least one party has the potential to lose through actions of another party that he trusts. The loss is not limited to monetary or financial loss, it can involve decrease in reputation, embarrassment when secrets or private information are revealed, breaking secrecy in nationally secret activities, a journalist revealing his sources, or a physician or priest breaking his seal of secrecy.

The first level of trust is created when personal direct interaction takes place between individuals. Trust can be created by observing a person’s behaviour toward you and others, does he show tact, is he telling stories about others, is he bragging, or does he reflect confidence and integrity? By observing his actions, having conversations with the other party and formal and informal correspondence with him, trust can develop. Formal correspondence has the advantage that in some cases it can be a basis for social or legal action in case the trust is compromised.

A second layer of trust is created through repetitive transactions with an individual, mainly transactions that involve financial and commercial activities such as buying and selling, when one party is the buyer and the other is the seller. A safe policy for developing trust is to begin with low dollar volume transactions; limiting possible damages to either party. If both parties come through on the limited transactions they can increase the volume of transactions or dollar value of their activity. Another example is trust compromising activities that can benefit the party holding the information, observing whether he compromises the trust. An example might be information that can make one employee look good by using information entrusted to him by another employee.

Trust is especially valuable when both parties have to lose if they break their mutual trust, for example through a reputation effect. Low reputation can influence others when dealing with the trader who broke financial or social trust. Such a dual effect reduces the incentives to breach trust for short term or low level gain.

Another mechanism to determine individuals' and companies trustworthiness is to initiate and collect information on their past trustworthiness. This can be achieved through the use of intermediaries who dealt with the other party in the past. Even when they are identified and used there are a number of possibilities:

1. If the intermediaries are personally known to the evaluator, he knows how much bias exists in their opinion, and how much weight to attach to their judgement; are they always lenient in their evaluation, or are they harsh? In addition he can ask and collect from them measurable data on the other party and their experience in dealing with him.
2. If the intermediaries and their characteristics are not known, information can be collected on their opinion worthiness. Care and judgement should be used as to what weight is assigned to their opinions, and if to contact them for their input, or not to contact them at all. Such a method is used in real life when a candidate for a job supplies references. It is unlikely that he will include in his list of references people who have a poor opinion of him. Even in such cases it is possible to overcome the initial bias by asking the references if they can recommend others who are not on his list who know him or for whom he has done work in the past. Such a method is used by security agencies to check individuals for security clearances for sensitive positions.

The other party can provide objective data that helps in determining if you want to do business with him. For example, current or past customers, financial data, annual reports, past delivery dates, quality measures, attrition rate of employees and managers. It is possible also to collect objective measures on past performance of the other party, such as bank records, membership in professional organizations, address and length of time in his line of business, etc.

An avenue open to test the honesty or trustworthiness of the other party can be achieved by proposing to him to take actions which are in the grey area of legality; for example, paying him under the table, offering a service or a favour (on the boundary of bribe). If the second party takes the bait, the initiator of the offer collects information on the level of honesty of the other party. The use of such an extreme method should be limited to very special cases, it has the danger of being a double sword method as it can reflect badly on the entity proposing such an action. Caution has to be undertaken when offering an action whose legality is questionable.

When the trading partner is an unknown entity, it is possible to shift the burden to him, by requiring that he shares the risk involved in the transaction. Examples include:

1. Payment after delivery, ask the other party to deliver before payment is made, i.e. ask the other party to fulfil their part of the agreement before you do your part. The danger here is that the other party takes the full risk, as the recipient may not pay at all after delivery took place.
2. The second party should provide a letter of credit from a bank, or an active credit card, so that he can be charged in case he does not deliver according to the agreement.

Let others share the risk (for a fee). This includes the use of escrow or insurance services, for example, paying a fee to a reputable agency that insures the transaction in case the other party does not fulfil his commitment. Another mechanism along the same lines is the use of

COD (Charge on Delivery) in which the delivery company is the one collecting the payment after the buyer has checked and verified that he received what he ordered.

Forming an opinion on the trustworthiness of someone in a commercial transaction is not easy even when the two parties operate in the same city, state or country. It becomes a lot more difficult when the trading parties are in different countries and continents. Issues such as different languages which might involve misunderstandings when translations take place; different cultures and customs which could be misinterpreted by the other party; different legal and financial institutional arrangements, for example who has legal authority in case of disputes? Other considerations are how to construct a contract acceptable in the two countries, who has the rights to intellectual property generated through the joint activity, and how to take into account the impact of future exchange rates.

3. Methods used by swindlers

Many methods are used by swindlers to defraud Internet users; in this section we concentrate on methods that swindlers use to defraud participants in auctions [2,4,9]. We present the main methods used and classify them:

1. *Non-delivery*: The swindler offers to sell items or provide services to the buyer; The buyer pays in advance before a tentative delivery took place, the swindler does not deliver anything to the buyer. Here there are several sub-cases:
 - A. *Delivery does not take place* at all and no refund is offered or made. The buyer is out the amount he paid. This is especially hurtful if payment was made using a non-recoverable method such as money order, cash, or some of the instant payment agencies.
 - B. *Delivery does not take place*, but the seller offers to refund the amount paid. The buyer is happy, he assumed that the money was lost, and finds out that the sum he paid will be returned to him. This is an interesting scheme as the swindler makes money at the expense of the buyer. There are several variants of this scheme:
 - i. The sum he paid is returned to him, typically in a check that he has to deposit. This scheme works in the following way.
 - 1) The seller offers to sell an expensive item worth a few thousand dollars. He states in advance that the actual shipment of the order will take place 45 days after full payment has been received.
 - 2) The buyer pays for his order. At which point the shipment clock is triggered
 - 3) The shipment does not take place within the promised time frame of 45 days.
 - 4) After some wait (typically 7 to 14 days), the buyer contacts the seller.
 - 5) The seller explains that due to manufacturing delays at the manufacturer site/s (or some other excuse), he could not deliver on time and offers the buyer to wait a few more weeks, or accept a full refund of his original payment.
 - 6) Many buyers decide to wait the extra time, the logic being, "I waited two months, what is the harm of waiting two or three more weeks?" Once the waiting period has passed, one of the following procedures takes place:
 - a) *No shipment takes place* and the buyer is refunded his money (typically 60 to 70 days after his original payment). The buyer does not complain as his payment was refunded. In this version the seller makes money from the

interest on the float. Auctioning around 25 products per day, for an average final price of \$2000, the amount of cash available to him for investment is $\$2000 \times 25 \times 60 = \$3,000,000$. Using a conservative interest rate of 5 percent per year, he earns around \$150,000 per year just on the interest, minus the administrative costs of receiving payments, handling the accounts and issuing refund checks, all of which can be fully automated.

- b) *Shipment takes place* of an alternate product with similar stated characteristics. Most buyers do not notice minor changes in the shipped product versus the advertised one. For example, the original product was suppose to have a Mobile Pentium 2 GHz. The seller delivers as a compensation for the long delay a “superior” product, with a faster processor of 2.4 GHz, but the buyer does not notice that it is a Pentium and not a Mobile Pentium; he loses mobility, and a difference of a few hundred dollars. If the buyer understands the consequences of such a switch, he can return the item for a full refund. However, based on reading the positive feedback from buyers who went through such a process, most of them do not detect or understand the difference. They accept the inferior product as a superior one and actually thank the seller for his “generous” service.
- c) *Shipment takes place* of the advertised or promised product. The sellers benefit in this case stemming from the observation that in many electronic products, prices decline by 3 to 5 percent per month. An item auctioned for \$2000, can be bought for around \$1850 two months later. The seller buys the item at the lower price and ships it to the buyer, pocketing the difference in price minus the shipping and transaction costs. In another variant of the same scheme, the seller (or his software agent) follows items auctioned or sold on multiple sites, when he discovers the same item he committed to sell, priced at a much lower price on another site; he buys it at the lower price, and provides his original buyer’s address as the shipping address of the product he bought.

It is difficult to argue the illegality of the above scheme, the seller disclosed most of the information beforehand and the buyer was a willing participant throughout the process. However, the buyer has the option of using a civil lawsuit to recover the damages caused by the delay, an option that buyers rarely exercise.

2. *Shipment and delivery takes place* but:

- a. An empty box or one containing worthless items is sent. There were cases in which stones or sand was delivered. The sellers were careful to make sure that the package had the same weight as a legitimate package. Having the same weight, the sellers could make the claim that they actually shipped the item. If the shipment was insured, the insurance company had to cover the cost of the item.
 - b. A partial shipment or substitute items are sent: for example, a laptop with a lower disk or memory capacity.
 - c. Damaged or non functional merchandise is shipped. If the shipment was insured, the insurance pays for the defective items, or if the item is still under the manufacturer’s warranty, the manufacturer repairs the defective item.
3. After the auction, a losing bidder receives an unsolicited proposal to sell him the same type of equipment he showed interest in or was bidding for, typically at a lower price than the winning bid. If the bidder responds to the solicitation, he is asked to pay through

Western Union, or mail a cashier's check. Once the check or transfer is cashed, nothing is mailed and the buyer is out the cash. Several variants of this method have been developed to handle suspicious buyers:

- a. If the buyer insists on using an escrow company, the seller sends back a message, agreeing to use an escrow company and provide the buyer with a link to an escrow company. Unfortunately, in several cases we checked, the escrow company was a fraudulent company set up by the swindlers.
 - b. If the buyer insists on using a specific shipping company (ABC for example), the seller agrees to it and provides a link to a legitimate looking shipping company. The barely detectable difference is that instead of www.ABCD.com the buyer is directed to www.ABCD.org, a different suffix set up by the swindlers. In all other respects the site appears identical to the legitimate company (the swindlers simply copy the legitimate site).
 - c. Specifying that they are from the US and a legitimate business, while payment is made to an overseas account. Once payment is made, the payee can forget about receiving his order. The crooks in this case benefit even if no payment is made. Once the potential victim has responded to the solicitation, his name and email address are sold to spamming lists, identifying him as an active email!
4. *Planted (skill) bidders in auctions*, Another method used in on-line auctions is for the seller to have a partner who bids up the price of an item being auctioned. This happens when the partner detects a buyer who is willing to raise the price of the item. At some price level, the partner stops bidding and the buyer pays a price higher than what he would have paid without a planted artificial bidder. Another possible outcome is one in which the buyer stops bidding before the partner bailed out. In this case the partner is the winner of the auction. If such a case occurs one of two scenarios take place:
- i. The partner does not pay, and the item is re-listed on the same or another auction site. The seller does not complain, and no bad ratings are set on either party.
 - ii. The seller sends an email to the "second" highest bidder, offering to sell him the item for his highest bid price. The seller offers an excuse, such as he had several copies of the item and was willing to sell a second one, or he was cheated by the winning bidder. In many cases the bidder decides to accept the offer, as by his bidding he signalled that he was willing to pay that price.
5. *The Quick Buck Method*: This is a scheme in which swindlers have the potential of collecting hundreds of thousands of dollars in 24 hours. The swindler lists hundreds of expensive items on an auction site; examples of expensive items include flat panel plasma TVs, or laptop computers. The items have the following characteristics: all of them have the same starting date and time, and each item is unique (it could be the same type of item, but from different manufacturers or different models). The reason for uniqueness is to reduce the likelihood that the auction site or consumers will detect that they were listed by the same person. None of the items has a reserve price. All the listed items have the same termination date and time. In the cases that we detected, the termination time was set exactly 24 hours after the listing time. We were wondering, why the 24 hours? One possible explanation is that auction houses state in advance that their quickest response time to complaints is 24 hours. The seller has an outstanding reputation score (Figure 2) which in most cases was created by selling in the month preceding the quick buck auction penny items such as stamps or baseball cards (Figure 3). He provides outstanding service on the penny

c) your credit card information.....

← [Back to your last item](#) [Home](#) > [Services](#) > [Feedback Forum](#) > **Member Profile**

Member Profile: (91 ★)

Feedback Score:	91	Recent Ratings:	
Positive Feedback:	98.9%		
Members who left a positive:	92		
Members who left a negative:	1		
All positive feedback received:	114		


	Past Month	Past 6 Months	Past 12 Months
positive	100	114	114
neutral	1	1	1
negative	1	1	1

Member since: Feb-28-04
Location: United States

[ID History](#)
[Items for Sale](#)

[Contact Member](#)

[Learn about](#) what these numbers mean. **Bid Retractions (Past 6 months): 0**



[Browse](#) [Search](#) [Sell](#) [My eBay](#) [Community](#)

Fig. 2 A seller with a perfect score

←

2003-04 TOPPS T.J. FORD ROOKIE CARD Item number: 4121641277

You are signed in

Bidding has ended for this item (sfergpack is the winner)

If you are **sfergpack**, [Sign in](#) for your status.

 Go to larger picture	Winning bid:	US \$0.50	<p>Seller information</p> <p>(91 ★)</p> <p>Feedback Score: 91 Positive Feedback: 98.9% Member since Feb-28-04 in United States</p> <p>Read feedback comments Ask seller a question View seller's other items</p>
	Ended:	Apr-03-04 06:01:13 PST	
	Start time:	Apr-02-04 06:01:13 PST	
	History:	1 bid (US \$0.50 starting bid)	
	Winning bidder:	sfergpack (2796 ★)	

Fig. 3 The item sold to create the positive feedback





















	<u>GATEWAY M275XL LAPTOP PENTIUM M 512 MB</u>	\$700.08	12	11 hours, 37 mins +
	<u>GATEWAY M275XL LAPTOP PENTIUM M 512 MB</u>	\$1,225.00	15	11 hours, 37 mins +
	<u>GATEWAY M275XL LAPTOP PENTIUM M 512 MB</u>	\$1,225.00	17	11 hours, 37 mins +
	<u>DELL INSPIRON 8100 LAPTOP P3 256MB CD-RW/DVD</u>	\$496.51	10	11 hours, 39 mins +
	<u>DELL INSPIRON 8100 LAPTOP P3 256MB CD-RW/DVD</u>	\$409.99	13	11 hours, 39 mins +
	<u>DELL INSPIRON 8100 LAPTOP P3 256MB CD-RW/DVD</u>	\$520.00	37	11 hours, 40 mins +
	<u>HP Pavilion ZD7058CL LAPTOP</u>	\$910.00	17	11 hours, 41 mins +
	<u>HP Pavilion ZD7058CL LAPTOP</u>	\$960.00	16	11 hours, 41 mins +
	<u>DELL INSPIRON 8100 LAPTOP P3 256MB CD-RW/DVD</u>	\$384.93	18	Apr-24-04 10:34:25 PDT
	<u>DELL INSPIRON 8100 LAPTOP P3 256MB CD-RW/DVD</u>	\$373.92	16	Apr-24-04 10:35:12 PDT
	<u>DELL INSPIRON 8100 LAPTOP P3 256MB CD-RW/DVD</u>	\$373.47	15	Apr-24-04 10:35:30 PDT
	<u>DELL INSPIRON 8100 LAPTOP P3 256MB CD-RW/DVD</u>	\$369.58	17	Apr-24-04 10:35:55 PDT
	<u>DELL INSPIRON 8100 LAPTOP P3 256MB CD-RW/DVD</u>	\$374.42	29	Apr-24-04 10:36:17 PDT
	<u>DELL INSPIRON 8100 LAPTOP P3 256MB CD-RW/DVD</u>	\$373.52	18	Apr-24-04 10:36:32 PDT
	<u>DELL INSPIRON 8100 LAPTOP P3 256MB CD-RW/DVD</u>	\$384.99	17	Apr-24-04 10:36:46 PDT
	<u>HP SB21 Digital Projector</u>	\$405.01	13	Apr-24-04 10:44:33 PDT
	<u>DELL INSPIRON 8100 LAPTOP P3 256MB CD-RW/DVD</u>	\$384.99	16	Apr-24-04 10:47:25 PDT
	<u>DELL INSPIRON 8100 LAPTOP P3 256MB CD-RW/DVD</u>	\$384.99	15	Apr-24-04 10:47:43 PDT
	<u>DELL INSPIRON 8100 LAPTOP P3 256MB CD-RW/DVD</u>	\$384.99	17	Apr-24-04 10:49:41 PDT
	<u>HP Pavilion ZD7058CL LAPTOP</u>	\$760.00	25	Apr-24-04 11:13:17 PDT

Fig. 4 Partial list of items put up for quick sale

items creating outstanding feedback for himself. This is preparatory work before he moves into the real deal (Figure 4). In one case we detected the listing of 160 items (Flat panel plasma TVs), the bids were in the range of \$2,000 to \$8,000 per item, netting the swindler \$400,000 to \$700,000 over a 24 hour window.

6. *Phishing* is a method used by swindlers to defraud innocent users of the Internet. The method is similar to hook and lure based phishing (this is the source of naming the method). When fishing the fisherman throws a hook with bait to the water, a fish (out of many potential fish) takes the bait and is hooked. Swindlers use a similar process: They send out a bait message as an email to thousands of innocent Internet users at a time.

A. The bait message states for example:

- 1) You won \$10,000 in a lottery, to deposit your lottery winning we need (for example):
 - a) your bank account information so that we can perform an electronic fund transfer.
 - b) your auction site account information (just the password)

- c) your credit card information
- 2) You have an account on the following auction site/payment system, the system was compromised, to make sure that your account is not among the compromised ones, please enter your password on the following message coming from that site.
 - 3) A government agency wants to verify your information, please enter your social security number, bank account information, etc.
 - 4) Your credit card was charged by mistake, to make sure that this was a legitimate transaction, please enter your credit card number, expiration date and name.
 - 5) We can sell you for bottom prices: Cheap medicine, pornographic materials, airline tickets, Please enter your credit card information so that we can charge the transaction.
 - 6) This is the police, your ID was stolen and to prevent unauthorized use of your card, please enter your credit card information.
- B. Some users bite the lure and “buy” the product or provide the information asked by the crook (the fisherman). Typically a very small portion of the users respond to the request (in the range of one out of a thousand).
- C. The next step is for the crook to get from the user information useful to his scheme. Once the information has been collected from several unsuspected users, the swindler establishes a temporary address, orders expensive merchandise online and charges it to the credit cards. The swindler asks for rush shipments (overnight if possible), picks up the items, sells them and disappears.
- D. It is difficult to track such crooks, as they use a similar process to collect networking account information from users, which are used later, sometimes several months after the collection.
- E. A swindler using the phishing method can collect large amounts of money per day even when a few of users respond and provide the information. In order to ensure a constant flow of income, the swindler has to constantly send out phishing messages to tens of thousands of users.

4. Fraud level in online auctions

Fraudulent activity that takes place before, during and after an auction is the most frequent incident reported to the IC3 data base (Smith [9]). Auction houses claim that fraud is rare and estimate it to be in the range of one incident per ten thousand to twenty thousand auctions. Such claims by auction houses should be taken with caution. Auction houses are not disinterested parties, their objective is to create the impression that fraudulent activity is very low and that bidders take a very low risk by bidding online. From casual observation of auction activity we were under the impression that the rate is higher.

Assuming that auction site claims of such a low level of fraudulent activity were true, trading activity can be encouraged by charging a minimal premium on each transaction. The collected premia can provide automatic insurance against fraud to the trading parties. If the above numbers are correct, a surcharge of one cent per ten dollars value of trade should suffice to provide trade insurance and significant profit to the insurance agency. That level of premia is a minuscule expense to the trading parties and leaves plenty of additional profit to the insuring entity. The increase in trading activity due to the peace of mind effect will attract more traders and will provide additional revenues to the auction houses. The fact that such

insurance is not offered at this level of premium casts doubt about the validity of claims of such low levels of fraudulent activity².

Providing low cost insurance is not as simple as it sounds. Having low cost automatic insurance can have an effect on the behaviour of the trading parties. One possible outcome could be an increase in their tolerance of higher levels of risk in their trading activity. This can lead to nonchalant attitude in their willingness to engage in trades when insurance is provided at low premium levels: they can undertake high risk trades with unknown parties. When such insurance is not offered, trading parties will be very careful in their trades and will not undertake that level of precarious activity. Another complication associated with providing negligible cost insurance is that it creates incentives for crooked traders to form coalitions in which they swindle the insurance agency. In spite of the potential for fraudulent trades, an insurance agency has many advantages over individual occasional traders in that due to the large number of trades that it monitors, it has the resources and experience needed to develop data bases, data collection and analysis systems, managerial and clerical procedures to detect and reduce such swindling activities to a minimal level. They also have the legal muscle to go after the crooks once criminal activity is detected. An economic advantage generated by low cost insurance premia is to encourage perceived high risk honest traders with no or limited trading history to enter the on-line trading community³. A positive outcome of such broader participation is that in addition to reducing the impact of fraud on the level of his own activities, the trader also benefits from a higher number of traders and a higher level of dollar volumes of activity.

In order to test the accuracy of the auction operators' estimates on the level of fraudulent activity, Gavish and Tucci [4] conducted a study on the magnitude of fraudulent activities in auction sites. Obtaining accurate numbers on fraud is difficult: traders who have been defrauded are hesitant to publicize the fact that they were careless and were defrauded; traders who were not defrauded do not have the incentive to respond to such surveys. The danger of being sued by the all powerful auction site operators is another hindrance to full disclosure of fraud information. In spite of the above difficulties and potential biases, the study established for each category of item classes a range on the number of fraudulent transactions that take place. The range estimates of the percentage of fraudulent activities are displayed in Figure 5. When we look at the overall estimate on the percentage of auctions with unsatisfied winners, they range from 21.4% for the most pessimistic estimate, to 1.76% for the most optimistic estimate. The large range of fraud related estimates follows from the way the estimate was computed. Only around ten percent of the questioners were returned by the sample⁴, we calculated the pessimistic estimate based on the data generated by the sample that actually responded, this could be an overestimate (i.e. people who felt strongly enough to induce them to respond), or an underestimate (eliminating people who feel embarrassed to admit that they were fooled). The optimistic estimate is one in which we assumed that all the people who did not respond had a positive experience and this is why they did not respond. It is interesting to note that even the optimistic estimate results in a fraud estimate of 1.76%; it is almost two orders of magnitude higher than what auction houses claim.

² Buyer insurance is offered on some auction sites for items that cost up to a few hundred dollars.

³ When tracking final bid prices on auction sites, we observed a price differential for the same item being auctioned, in favor of traders with an established history. In some cases the price differential reached up to \$500 on items in the \$1500 to \$2000 range. We observed a premium of 15 to 20 percent when comparing reputable vendors to vendors with no history.

⁴ This is a typical response rate to online questionnaires.

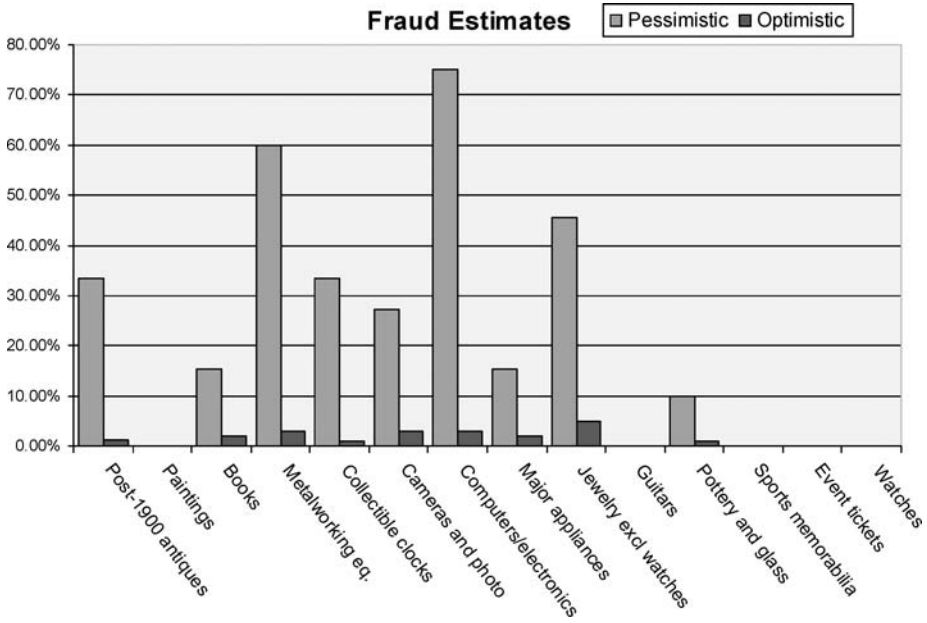


Fig. 5 Estimating the number of auction based transactions that are fraudulent

The study concentrated on buyers that are being defrauded. During the study we discovered that sellers face a similar problem of fraud. The main difference is that auction houses have developed extensive methods for protecting sellers, but limited effort went into protecting buyers. We conjecture that it has to do with the fact that if sellers do not put items up for bid, the auction site cannot survive, while bidders/buyers on their own cannot force the elimination of an auction site. Another factor working in favour of the sellers has to do with the frequency of use of the auction site. Most sellers use the auction site multiple times (in some cases, tens of thousands of times). Given a very high level of a single entity participation in auctions justifies seller’s investment in developing systems and methods that protect them against fraud. A buyer on the other hand has limited experience with the auction process and has limited knowledge as to how to protect himself against fraud, a distinct advantage for the seller.

5. Recommendations

The findings in Gavish and Tucci [4] and in Snyder [10], although preliminary, indicate a source of concern for traders (sellers and buyers) on the Internet. Even though the number of traders has been rising steadily for the last several years, it would not take much of a jolt to start the cycle in reverse [4]: buyers who become afraid that they will not receive the item they bid and paid for will stop participating in commerce activities, which means fewer buyers, which means fewer sellers, and so on. To reduce the likelihood for such a vicious cycle taking place, we have several recommendations based on the above studies.

- The more information is disclosed on sellers (and buyers) the higher is the degree of confidence in the system. A significant amount of data is collected by the auction houses,

posting some of it will enhance the validity of transactions that take place on the site. Here is some of the information that should be posted:

- The percentage of positive responses relative to the number of transactions for sellers (some sites have in 2003 begun to do this) rather than the absolute number.
- As mentioned above, some sellers sell (or buy) a large number of cheaper items to establish their reputation. To combat this problem, we recommend to publish the average selling price (or the full distribution of selling prices) of all previous auctions offered by the seller. Even better would be to divide it by months.
- Publish separate statistics for selling activity and for purchasing, thus reducing the chances that someone can establish a positive reputation simply by buying many low cost items.
- Indicate the number of distinct users that participated in creating a reputation history for a seller.
- Statistics on the percentage of cases in which seller was not paid, or buyer did not pay.
- Percentage of cases in which there was no response after the auction.

Trading sites should make the use of escrow services extremely easy, and possibly mandatory. Further, the buyer/seller should only use escrow services that are certified by the auction house. To that effect, auction sites should display the list of escrow services that they have certified with a URL to the sites.

Develop appropriate insurance policies that encourage electronic commerce activities. The premia should be at a reasonable rate, and the mechanisms should be designed to prevent collusion.

Auction houses can reduce the level of fraud by listing information on the seller, for example listing the physical (not electronic) address to which the payment will be made at the end of the auction. Having physical information can help a bidder in deciding if this is a legitimate seller or a swindler. In addition, the Internet provides tools that help in determining if such a seller does exist or if it is only a virtual seller.

The study reported here is based on a sample of around 1200 questionnaires; they were generated by hand by students contacting winners of auctions on an online auction house. A much larger sample size is needed in order to increase the validity of the conclusions. We are moving ahead with a much larger sample and will report its conclusions once the second study is completed.

References

- [1] BBC News, (1999). "The growing threat of internet fraud".
- [2] Cassell J., & Bickmore, T. (2000). "External Manifestations of Trustworthiness in the Interface", *Communications of the ACM*, 43(12), 50–56.
- [3] Cheskin, (1999). Research and Studio Archetype/Sapient Report, "E-Commerce Trust Study", <http://www.sapient.com/cheskin>.
- [4] Gavish B., & Tucci, C. L. (2003). "Swindlers and Buyer dissatisfaction in Internet auctions," Working paper, Ecole Polytechnique Fédérale de Lausanne, College of Management of Technology.
- [5] Knack, Keefer, S., P. (1997). Does social capital have an economic payoff? A cross-country investigation. *Quarterly Journal of Economics* 112(4), 1251–1288.
- [6] Kollock, Peter. (1994). "The Emergence of Exchange Structures: An Experimental Study of Uncertainty, Commitment, and Trust." *American Journal of Sociology* 100(2), 313–345.
- [7] Putnam, Robert D. (1993). "Making Democracy Work: Civic Traditions in Modern Italy." Princeton University Press.

- [8] Reuters. (2003). "Scam artists make hay on online auction sites." Reuters wire service, http://www.curztech.com/news/news/2003110_06.shtml, viewed 7/13/03.
- [9] Smith, Kaukab, J., (2005). "Online auction sites generate most Internet fraud cases," *The Capital*, Annapolis, Md.
- [10] Snyder, J. M. (2000). Online auction fraud: Are the auction houses doing all they should or could to stop online fraud? *Federal Communications Law Journal*, 52(2), 453–472.
- [11] VeriSign., (2003). "Internet Security Intelligence Briefing."
- [12] Waters R., (2003). "How fraudsters set traps and take the credit." *Financial Times*, IT Review, p. 1.

Bezalel Gavish holds the Eugene J. and Ruth F. Constantin Distinguished Chair in Business at the Edwin L. Cox School of Business at the Southern Methodist University in Dallas, Texas. Professor Gavish is the founding Chairman of the International Conference on Telecommunications Systems Management and the International Conference on Networking and Electronic Commerce. He is the Editor-in-Chief of the Telecommunication Systems Journal, and of the Electronic Commerce Research Journal. Professor Gavish was and is a consultant to numerous corporations and government agencies such as: IBM, AT&T, BNR, GTE, British Telecomm, MCI, Motorola, Xerox, Gorca Telecomm, the World Bank and others. His research interests include the design and analysis of computer communication networks, design and analysis of distributed computing systems, Fraud on the Internet, modeling of search processes on the Web, group decision support systems and their implementation, combinatorial optimization, and scheduling and routing in manufacturing and logistic systems. His research in telecommunications and computer networks concentrates on the topological design of wide area networks, Fiber deployment and design and analysis of local access networks, capacity assignment and routing in backbone networks, configuring cellular phone systems, analysis of low earth orbit satellite systems, economic and organizational impact of telecommunications and electronic commerce.

Christopher L. Tucci is Associate Professor of Management of Technology at the Ecole Polytechnique Fédérale de Lausanne (EPFL), Switzerland, where he holds the Chair in Corporate Strategy & Innovation. He received the Ph.D. in Management from the Sloan School of Management at the Massachusetts Institute of Technology. His prior work experience was as an industrial computer scientist at Ford Aerospace, where he was involved in developing Internet protocols in the 1980s. Dr. Tucci's primary area of interest is in technological change and how waves of technological changes affect incumbent firms. He is also studying how the technological changes brought about by the popularization of the Internet affect firms in different industries. He is the co-author of *Internet Business Models and Strategies*, and has published articles in, among others, *Strategic Management Journal*, *Management Science*, *IEEE Transactions on Engineering Management*, *Research Policy*, and *Journal of Product Innovation Management*. In 2004, he was elected to the five-year division leadership track of the Academy of Management's Technology and Innovation Management Division.