International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol.2, Issue.6, Nov-Dec. 2012 pp-4396-4404 ISSN: 2249-6645

Online Business Frauds: A Case Study of an Online Fraud Survey Company

PROF (DR) YASHPAL SINGH BIST[1], DR CHARU AGARWAL, [2]
UTTARA BANSAL, [3]
[1]*Professor faculty of mngt studies, Daas College of Mngt & Tech Dehradun (UK),*
[2, 3]*(Associate Professors, Deptt of computer science, Daas College of Mngt & Tech Dehradun (UK).*

ABSTRACT: *"Fraud and falsification are highly destructive to market capitalism and, more broadly, to the underpinnings of our society. Our market-system depends critically on trust. Trust in the word of our colleagues and trust in the word of those with whom we do businesss"*
----Alan Greenspan

The relationship between a customer and a business organization can stand only on the pillars of trust, faith, fair dealing and mutual expectation. Remove any pillar and the business will collapse but in the great Internet fraud factory these pillars are non-existent. Just a Google search for "internet fraud" pops out 26 lacks results in less than 28 sec indicating the huge menace the global networked world is facing, it's a vicious cycle of greed, ignorance and fast money, which prods the victims to believe in these surreal scams, they invest their hard-earned money and time. The fraudsters spin their web of lies and deceit, dangling the lure of easy money and false commitments they wait to devour their victim of their self esteem and trust, brutally savaging their faith in the internet, worst still in majority of cases the victims have no redressal' mechanism in their country as where to complain since these fraudsters leave no physical and legal footprints .The onus no doubt lies with the unsuspecting victims but its also up to the various countries to make their legal IT Laws stringent and strong so that these fraudsters are treated as global frauds and be strictly dealt with. Government organizations and NGO's should educate the netizens on the "human trust" traps laid for them on the information superhighway. This paper deals with the various dubious mechanisms of fraudulent solicitations made by internet fraudsters, what can be done and why do we fall for it. We specially investigate the online survey frauds.

Keyword: *Business Ethics, Internet fraud, Investment frauds, Business frauds, Online survey fraud, Nigerian letter fraud, Fraud management system*

THE BROAD CATEGORIES OF INTERNET BASED SCAMS ARE

I. Investment related internet scams

(a) Online auction and retail schemes
(b) Online Survey frauds

II. Business Fraud:

(a) Purchase frauds
(b) Online automotive fraud
(c) Counterfeit cashier's check scam
(d) PayPal Fraud
(e) Call tag scam
(f) Money transfer fraud
(g) Target youth frauds

III. Target elder fraud

(1)Investment related internet scams:

(a)Online auction and retail schemes
(b)Online survey frauds

(a)In an *online auction scheme*, a fraudster starts an auction on a site such as eBay or TradeMe with very low prices and no reserve price, especially for typically high priced items like watches, computers, or high value collectibles. The fraudster accepts payment from the auction winner, but either never delivers the promised goods, or delivers an item that is less valuable than the one offered—for example, a counterfeit, refurbished, or used item.

Online retail schemes, involve complete online stores that appear to be legitimate. As with the auction scheme, when a victim places an order through such a site, their funds are taken but no goods are sent, or inferior goods are sent. However the eBay Site has introduced certain financial control mechanisms and thus until the user is not satisfied with the product the seller will not get the money and in case even after15 days the buyer fails to inform ebay, ebay believe that the product payment.

Fraud Management in the online retail environment:

A staggering 28% of all online retail orders are affected by fraud[2] .This has direct impact on the ecommerce profitability, operating efficiency and scalability .G.S Paintal of Infosys in his white paper "Fraud Management in the online retail environment" Recommends the following security steps:

1) Online payments authorizations of credit cards (This ensures that the card is not stolen or lost and has enough credit in it)
2) Address Verification services (AVS) (It Checks billing address of customer with the billing address in the card)
3) Use of card verification code (CVV.CVV2)(its 3 or 4 digit number printed at the backside of credit card and ensures that the card was physically present at the time of purchasing)
4) Negative files (it consists of a file having data of stolen cards, fake addresses, hacked emails etc)
5) Risk predication models/Electronic data warehousing system (Here special soft wares are used which analyzes data from millions of online sales and each prospective order is run through this algorithm and checked for any suspicious attributes)
6) Manual reviews (It's the same as above but is done manually, its time consuming)
7) Verified by Visa/Master card secure code (these have advanced security mechanisms which take onus of the transactions)

According to Paintal we must have a well modular architecture which clearly defines:

(1) Ecommerce store front 2) Payment gateways 3)order management system 4)fraud management system and electronic data ware housing analytics

(b) Online Survey frauds:

The question is are there any online survey companies which are genuine, Yes, but its almost impossible to find, a Google search of "online surveys" prompts out 77,3000 results. But in case you are interested be cautious, according to audri and Jim of *Internet ScamBusters™*, ignore all spam solicitations. They are all scams. Secondly, use a search engine to see if you can find info on the company, including complaints[3.] ASIAN countries like India, Bangladesh, Nepal etc have recently witnessed a surge in ONLINE SURVEY FRAUDS notably **Speakasia** has swindled huge amounts of money. Home Minister R R Patil of Maharastra said the Speakasia fraud could be as big as Rs 2,000 crore and the money sent out of the country. The minister cautioned people against investing money in companies which make unbelievable promises and said economic offences to the tune of Rs 699.70 crore were reported in the state in 2010 alone.

Patil said cases had been reported against the Singapore-based company in other parts of the world and added that about 20 lakh people could have been duped in all. "We acted as soon as we received a complaint in the matter[4]

Speak Asia was registered in Singapore, and it costs nothing.

Company Background:

The company name is: SpeakAsia Online Pte Ltd.

formerly known as : Haren Technology Pte. Ltd.

Earlier known as: PAN Automotives Pte. Ltd

(Compliance rating for this company is Non Compliant currently)

Prior to this name they were operating under:

HAREN VENTURES PTE. LTD.

Formerly HAREN AUTO PARTS PTE. LTD.

Formerly HAREN MULTICONSULT TRADE SERVICES PTE. LTD.

Search found <8> matches
Displaying Page <1> of <1>

S/No.	Registration No. Click below hyperlink to buy entity information.	Entity Name	Partial Address	Status	Compliance Rating for Annual Filing Click on icon for details of compliance records.
1	53023024X	HAREN AUTO & HEAVY EQUIPMENTS **f.k.a** HAREN AUTOMOTIVES & COMPONENTS	EMERALD HILL ROAD	Cancelled	-
2	52885731B	HAREN MULTICONSULT TRADE SERVICES	CHIN SWEE ROAD	Terminated	-
3	200613527C	HAREN VENTURES PTE. LTD. **f.k.a** HAREN AUTO PARTS PTE. LTD. **f.k.a** HAREN MULTICONSULT TRADE SERVICES PTE. LTD.	BUKIT BATOK CRESCENT	Live	✓
4	53034470W	HARENA ENTERPRISE	JALAN SULTAN	Live	-
5	200705083Z	HARENA PTE. LTD.	LORONG 23 GEYLANG	Struck off	-
6	52998195E	HARENE'S	RACE COURSE ROAD	Cancelled	-
7	35495100M	HARENRA STORE	YISHUN STREET 71	Terminated	-
8	200618809D	HAREN TECHNOLOGY PTE. LTD. **n.k.a** SPEAKASIA ONLINE PTE. LTD. **f.k.a** PAN AUTOMOTIVES PTE. LTD.	UBI CRESCENT	Live	✗

Notes:
1. **n.k.a** means "now known as"
2. **f.k.a** means "formerly known as"
3. Compliance rating is available for "Live" companies only.
4. Compliance tracking for the company is based on real-time information.

Source: www.psi.gov.sg

a) There is a defunct website too http://www.hmtservices.com where we can see is that there is no relation between the survey they used to do for products ,also in the link spare parts there is no mention of any product obviously it was all a fake website.

b) When doing little more research on the address of the company the same address is used for different companies. A simple Google can throw a few names which I am listing below. Some of the companies having the same address are: Valves.Com Pte Ltd, SBS Consulting Pte. Ltd.

c) The company has a franchisee model so at the face of it you are not paying anything directly to the company "Speak Asia" and it goes in the name of the franchise (bank account) and who further pass that money to someone in Mumbai and all get to keep a certain % out of it.

If it's such a big company they should provide an option to pay online through credit card directly to them instead of making so many layers of people accepting payments on company's behalf and would have helped them with instant signups.

d) If you watch YouTube for their Torch Bearers 2011 meet they were talking about opening a TV Channel by August 2011. Very nice and ambitious plan but doesn't it require a lot of regulatory processes and time and huge "money". But the ground reality is that they don't have a single registered office in India. There are claims that it will be open in May 2011 in Mumbai.

e) We found that they were using SurveyMonkey as their survey tool and only recently purchased Novi Survey. However established proven businesses with multi million dollars in revenue build there own software tools in-house.

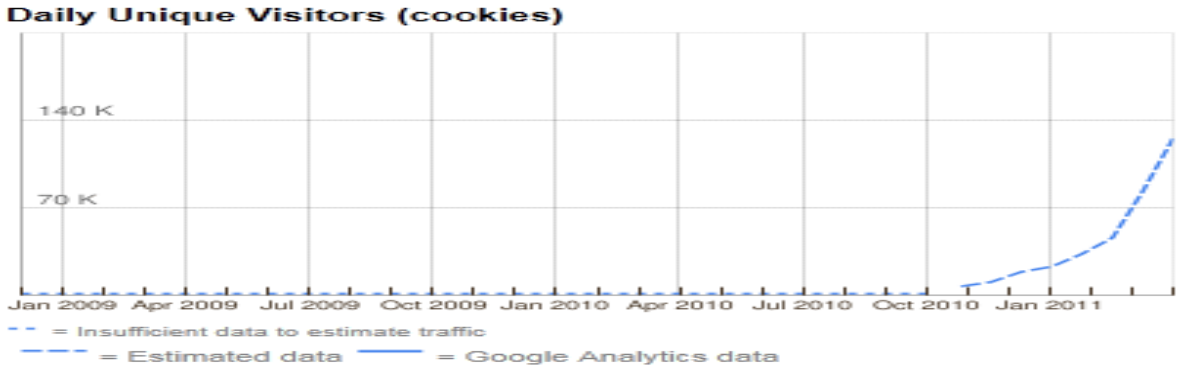
f) They claimed they were getting good business in Singapore / Malaysia / Indonesia but after searching the Alexa site we find that the traffic is mainly in India and Bangladesh only.

Screenshot from Alexa:

Speakasiaonline.com's Regional Traffic Ranks

Country	Rank
Bangladesh	43
India	91

The below screen shot shows the amount of traffic per day in speakasia website



The traffic in India

View data for: India

Traffic statistics All traffic statistics are estimates

	Country	Worldwide
Unique visitors (estimated cookies)	990K	990K
Unique visitors (users)	910K	920K
Reach	1.6%	0.0%
Page views	98M	110M
Total visits	3.9M	4.2M
Avg visits per visitor	4.2	4.6
Avg time on site	21:40	21:40

g) Speak asia advertised heavily on IPL matches, daily newspapers, the celebrities were not even paid in full[5]

h) Again when you do some research on the domain: SpeakAsiaOnline.com

this was registered on **21 January 2010** and they started working in India from February 2010. So the point is that the whole scheme is not that OLD as the company proclaims that it is working since 2006. Earlier the company was doing agreements with Franchisee through the name "Haren Auto Parts Pte. Ltd.", which again changed to Haren Ventures Pte. Ltd.

Registrant:
Speakasia Online Pte. Ltd.

71 Bukit Batok Crescent #10-08 Prestige
Singapore, 658071
Singapore

Registered through: GoDaddy.com, Inc. (http://www.godaddy.com)
Domain Name: SPEAKASIAONLINE.COM
Created on: 21-Jan-10
Expires on: 21-Jan-13
Last Updated on: 06-Nov-10

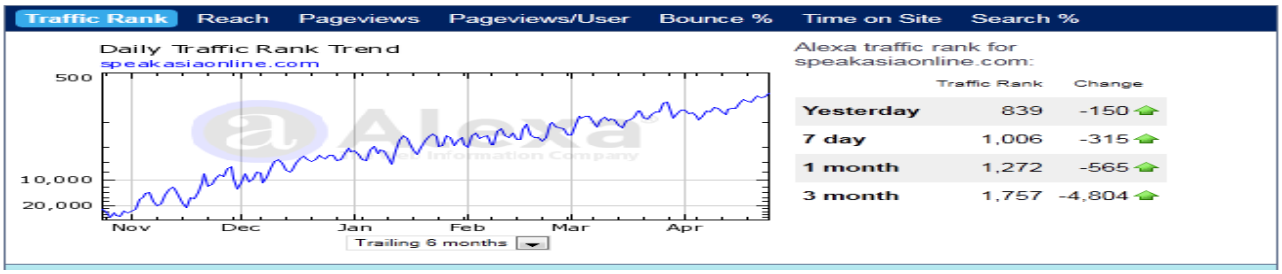
Administrative Contact:
asia, speak support@speakasiaonline.com
Speakasia Online Pte. Ltd.
71 Bukit Batok Crescent #10-08 Prestige
Singapore, 658071
Singapore
+65.91234567

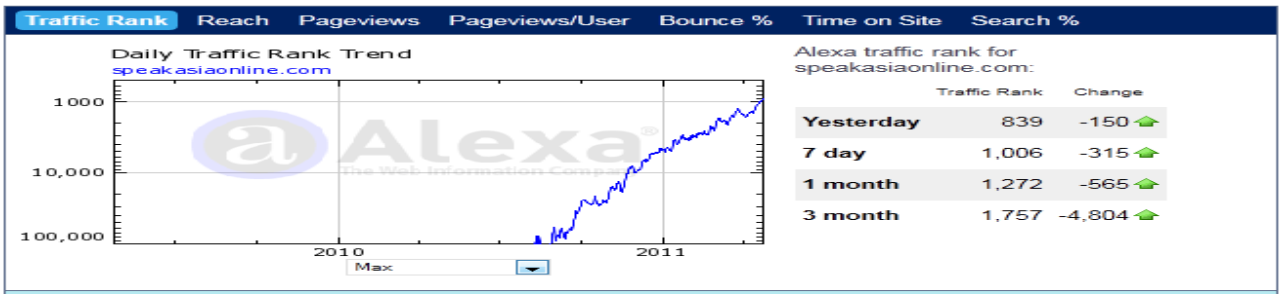
The address mentioned on their WHOIS doesnt match with their registered company address.
WHOIS Record says:

Speakasia Online Pte. Ltd
.71 Bukit Batok Crescent #10-08 Prestige
Singapore, 658071
Singapore
Company website mentions:

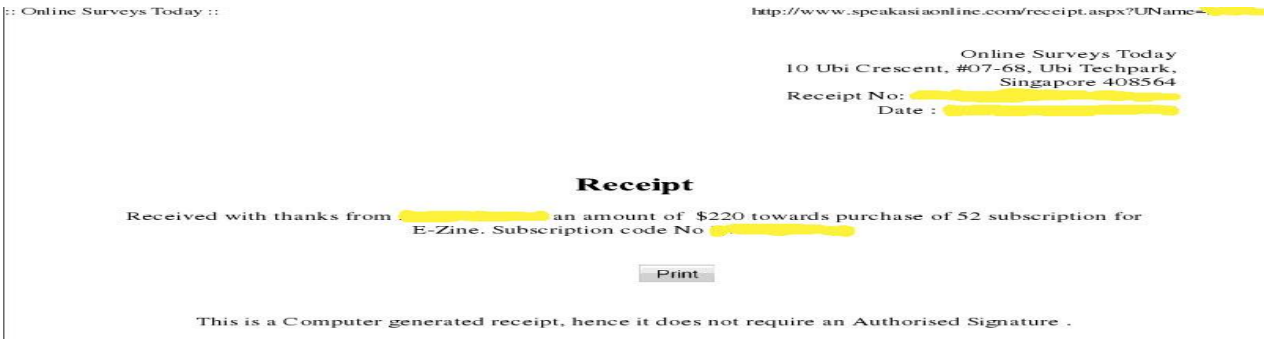
Speak Asia Online Pte. Ltd.
Address: 10 Ubi Crescent, #07-68, Ubi Techpark,
Singapore 408564

h) The site indeed got a lot of traffic and that certainly makes them one of the fastest growing website, their current Alexa ranking is at 839 (as on april 2011)





i) Speakasia was like a Ponzi scheme
. For the first three month it is actually paid from its pocket and after that since users had obviously multiplied they started getting more money as planned by them.
j) legal problems: Speakasia knew that since the company was registered in Singapore thus in order to recover 11000 Rs one would have to go to Singapore to file case which as we can comprehend will be not feasible , secondly the company was selling E-Zine and the victim had paid 11000 towards that and not towards the Survey. Your payment of Rs.1000 / 2 surveys is toward the Surveys you fill. So on that ground too the company is safe
k) Yes one do receive a online reciept for the money that one pays from Speak Asia and here is the screenshot. Earlier it was given from "Online Surveys Today" which I doubt that any such company even exists though the address was same as SpeakAsia Online Pte. Ltd. and later it is changed to Haren Ventures Pte. Ltd.but they had later changed the address to a new address ,see screen shots below


:: Online Surveys Today ::

http://www.speakasiaonline.com/receipt.aspx?UName=

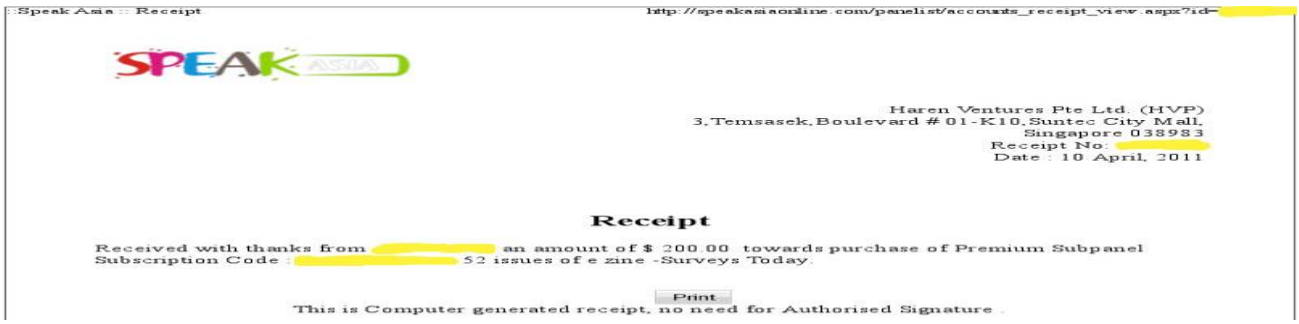
Online Surveys Today
10 Ubi Crescent, #07-68, Ubi Techpark,
Singapore 408564
Receipt No:
Date :

Receipt

Received with thanks from an amount of $220 towards purchase of 52 subscription for E-Zine. Subscription code No

Print

This is a Computer generated receipt, hence it does not require an Authorised Signature .


::Speak Asia :: Receipt

http://speakasiaonline.com/panelist/accounts_receipt_view.aspx?id=

Haren Ventures Pte Ltd. (HVP)
3,Temsasek,Boulevard # 01-K10,Suntec City Mall,
Singapore 038983
Receipt No:
Date : 10 April, 2011

Receipt

Received with thanks from an amount of $ 200.00 towards purchase of Premium Subpanel Subscription Code : 52 issues of e zine -Surveys Today.

Print

This is Computer generated receipt, no need for Authorised Signature .

References (http://blog.investraction.com/2011/04/speak-asia-scam-or-for-real.html,
http://www.suchetadalal.com/?id=90890ade-4fcf-f284-4da58466269d&base=sections&f,
http://www.moneylife.in/article/speakasia-still-cant-show-valid-legal-documents/15551.html
http://www.aboutindiatoday.gen.in/2011_02_01_archive.html
http://timesofindia.indiatimes.com/city/nagpur/Another-co-goes-to-town-with-easy-money-scheme/articleshow/7523895.cms
Things to know before making money from online surveys firms article appeared on The economic times on 09/05/2011
What could have been done: The Indian government should have woken up to the fact that the advertisements were released in all leading print and broadcast media and every govt department ,be it vigilance ,or
(2) Business Fraud:

(a)Purchase frauds

Purchase fraud occurs when a criminal approaches a merchant and proposes a business transaction, and then uses fraudulent means to pay for it, such as a stolen or fake credit card. As a result, merchants do not get paid for the sale. Merchants who accept credit cards may receive a chargeback for the transaction and lose money as a result.

(b)Online automotive fraud

A fraudster posts a nonexistent vehicle for sale to a website, typically a luxury or sports car, advertised for well below its market value. The details of the vehicle, including photos and description, are typically lifted from sites such as eBay Motors or Autoscout24. An interested buyer, hopeful for a bargain, emails the fraudster, who responds saying the car is still available but is located overseas. The scam artist then instructs the victim to send a deposit via wire transfer to initiate the "shipping" process. The unwitting victim wires the funds, and subsequently discovers they have been scammed.

(c) Counterfeit cashier's check scam

Landlords placing advertisements on Craigslistrent.com receive an e-mail response from a prospective renter from a foreign country, typically a student fresh out of secondary education (high school in the U.S.). The first inquiry seems legitimate. The second usually comes with request for more information and an attachment from a fake company set up by the scam artist indicating that the "student" has won a part-time scholarship from the company. (The fraudster will often set up a fake website for the company, in order to make the attachment seem legitimate.) The scam comes with the third e-mail: a request for the victim's name and address so that the "company" can send a cashier's check to cover the rent and the "student's" travel costs.

The victim is instructed to cash the check and wire the difference back to the student so that they can travel to the destination country. In the United States, banks consider cashier's checks to be "guaranteed funds" and will typically cash them instantly. However, unlike a certified check, the bank that cashes a cashier's check can still take back the money from the depositor if the check is counterfeit or "bounces". Because of the lag between the cashing and clearing of the check, the victim does not realize that they have been had until their account is debited for the amount they wired to the fraudster, plus any fees for the bounced check.

(d)PayPal Fraud

In a **collection in person PayPal scheme**, the scammer targets eBay auctions that allow the purchaser to personally collect the item from the seller, rather than having the item shipped, and where the seller accepts PayPal as a means of payment.

The fraudster uses a fake address with a post office box when making their bids, as PayPal will allow such an unconfirmed address. Such transactions are not covered by PayPal's seller protection policy. The fraudster buys the item, pays for it via PayPal, and then collects the item from the victim. The fraudster then challenges the sale, claiming a refund from PayPal and stating that they did not receive the item. PayPal's policy is that it will reverse a purchase transaction unless the seller can provide a shipment tracking number as proof of delivery; PayPal will not accept video evidence, a signed document, or any form of proof other than a tracking number as valid proof of delivery .This form of fraud can be avoided by only accepting cash from buyers who wish to collect goods in person.

(e)Call tag scam

In a call tag scam, criminals use stolen credit card information to purchase goods online for shipment to the legitimate cardholder. When the item is shipped, the criminal receives tracking information via email. They then call the cardholder and falsely identify themselves as the merchant that shipped the goods, saying that the product was mistakenly shipped and asking permission to pick it up when it is delivered. The criminal then arranges the pickup, using a "call tag" with a different shipping company. The victim usually doesn't notice that a second shipping company is picking up the product, and the shipping company has no knowledge it is participating in a fraud scheme.
The cardholder may later notice the charge on his statement and protest the charge, generating a chargeback to the unsuspecting merchant

(f)Money transfer fraud: consists of an offer of employment transferring money to a foreign company, supposedly because it costs too much to do it through other methods. The prospective victim receives an email like
Dear Sir/Madam I'm the C.E.O of XXXXX Textiles. We'd like to offer you additional earnings $2000 – $8000 per month. It's easy and will not take a lot of time. No costs, No Investments, Work Part Time or Full Time. Up to $2000 Part Time and $8000 Full Time. Work from Home with a Business Opportunity that no job could ever offer. Use your own computer to make money and make a CAREER as your own boss. I would like to know if you are interested. Work will consist of receiving of the payments from our clients in USA and Canada. All you would be doing is receiving these payments that would come to you via the mail system in your country, have them cashed and remit the rest to me. I would be willing to pay you 10% of whatever payment you process. These payments would come in different forms. We are always facing serious difficulties when it comes to selling our products to Americans; they are always offering to pay with Different Modes, which are difficult for me to cash here in the UK. Because of a hold of almost three weeks that would be placed on them before they clears the banks here in the UK. Unfortunately we can't open the bank accounts in all the countries we work with and because of that we seek for a representative/bookkeeper in USA and Canada. Respond only if you will like to work from home part-time/full time and get paid weekly without leaving or it affecting your present job. (PAY IS GOOD)If interested please reply with the information below to

Email: XXXXXX@XXXXXX.com EMPLOYMENT APPLICATION FORM:
FULL NAME.....
ADDRESS (P.O Box Not Accepted).....
CITY.....STATE....ZIPCODE....
PHONE..... CELL PHONE.....
AGE.....SEX.....
PRESENT OCCUPATION.....
RECENT BANK..... XXXXXXX XXXXXXXX ARTS AND CRAFTS
99-98 XXXXXX STREET XXXXXXXXXX
LONDON,WG2B 6TD
+44-999-999-9999 Best Regards,
Mr. XXXXX XXXXX

The fraudsters then send fake checks or postal money orders, in the hopes that the victims will cash the fake money instruments and send money to the scammers before the fraud is discovered.
Because the fraudsters are often able to get the victim's personal information, including their Social Security number or bank account number, these scams often become phishing scams as well, leading to identity fraud.

Why can't a pyramid scheme work?

The fact that a pyramid scheme cannot work for all, or even most participants can be proven mathematically and shown by this example:
This table shows how many new paying members must be recruited at each level for programs (schemes) that require each new member to recruit 4, 5, 6, 7, or 8 new members.

Level	Each person must recruit Members that must be recruited by each level (total) to be profitable for that level if each member must recruit the following new members:				
	4	5	6	7	8
1	4	5	6	7	64
2	16	25	36	49	512
3	64	125	216	343	4096
4	256	625	1,296	2401	32,768
5	1,024	3125	7,776	16,807	262,144
6	4,096	15,625	46,656	117,649	2,097,152
7	16,384	78,125	279,936	823,543	16,777,216
8	65,536	390,625	1,679,616	5,764,801	134,217,728
9	262,144	1,953,125	10,077,696	40,353,607	1,073,741,824
10	1,048,576	9,765,625	60,466,176	282,475,249	8,589,934,592
11	4,194,304	48,828,125	362,797,056	1,977,326,743	68,719,476,736
12	16,777,216	244,140,625	2,176,782,336	13,841,287,201	
13	67,108,864	1,220,703,125	13,060,694,016		

You will notice that the reddish colored cells signify levels that are unachievable because there aren't that many people on earth (approximately 6 billion people)! The orange colored cells signify levels that are practically unachievable: there are no existing companies on earth with this many employees or members. The yellow colored cells indicate levels that are mathematically possible, but would mean that the company would be huge by most standards (7,000 to 1 million employees) and this is VERY unlikely. The uncolored cells are levels that are possible and maybe even practically achievable - by really good con men! This does NOT mean that we are recommending them.

IV. Target youth frauds:

(a) **Internet ticket fraud**
(b) **Nigerian letter 419 fraud.**

(a)Internet ticket fraud

A variation of Internet marketing fraud offers tickets to sought-after events such as concerts, shows, and sports events. The tickets are fake, or are never delivered. The proliferation of online ticket agencies, and the existence of experienced and dishonest ticket resellers, has fueled this kind of fraud. Many such scams are run by British ticket touts, though they may base their operations in other countries. A prime example was the global Beijing Olympic Games ticket fraud run by US-registered **Xclusive Leisure and Hospitality**, sold through a professionally-designed website, www.beijingticketing.com, with the name "Beijing 2008 Ticketing". On 4 August it was reported that more than AU$50 million worth of fake tickets had been sold through the website. On 6 August it was reported that the person behind the scam, which was wholly based outside China, was a British ticket tout, Terance Shepherd.

(b) **Nigerian letter 419 fraud:** Nigerian letter frauds combine the threat of impersonation fraud with a variation of an advance fee scheme in which a letter mailed from Nigeria offers the recipient the "opportunity" to share in a percentage of millions of dollars that the author—a self-proclaimed government official—is trying to transfer illegally out of Nigeria. The recipient is encouraged to send information to the author, such as blank letterhead stationery, bank name and account numbers, and other identifying information using a fax number provided in the letter. Some of these letters have also been received via e-mail through the Internet. The scheme relies on convincing a willing victim, who has demonstrated a "propensity for larceny" by responding to the invitation, to send money to the author of the letter in Nigeria in several installments of increasing amounts for a variety of reasons.

Payment of taxes, bribes to government officials, and legal fees are often described in great detail with the promise that all expenses will be reimbursed as soon as the funds are spirited out of Nigeria. In actuality, the millions of dollars do not exist, and the victim eventually ends up with nothing but loss. Once the victim stops sending money, the perpetrators have been known to use the personal information and checks that they received to impersonate the victim, draining bank accounts and credit card balances. While such an invitation impresses most law-abiding citizens as a laughable hoax, millions of dollars in losses are caused by these schemes annually. Some victims have been lured to Nigeria, where they have been imprisoned against their will along with losing large sums of money. The Nigerian government is not sympathetic to victims of these schemes, since the victim actually conspires to remove funds from Nigeria in a manner that is contrary to Nigerian law. The schemes themselves violate section 419 of the Nigerian criminal code, hence the label “419 frauds.”

V. Miscellaneous interent frauds :

(a) **Phishing**

(b) Pharming

(a) **Phishing**

Phishing is the act of masquerading as a trustworthy person or business to fraudulently acquire sensitive information, such as passwords and credit card details, that a victim might think reasonable to share with such an entity. Phishing usually involves seemingly official electronic notifications or messages, such as e-mails or instant messages. It is a form of social engineering.

Fraudsters have widely used e-mail spam messages posing as large banks like Citibank, Bank of America, or PayPal in phishing attacks. These fraudsters copy the code and graphics from legitimate websites and use them on their own sites to create legitimate-looking scam web pages. These pages are so well done that most people cannot tell that they have navigated to a scam site. Phishers will also add what appears to be a link to a legitimate site in an e-mail, but use specially-crafted HTML source code that actually links to the scammer's fake site. Such links can be often revealed by using the "view source" feature in the e-mail application to look at the destination of the link, or by putting the mouse pointer over the link and looking at the URL then displayed in the status bar of the web browser. **Examples of phishing attacks**[7]

Subject: Windows Account Alert™

From: Windows Microsoft™ Center (war.veteran@hotmail.com)

Sent: Fri 4/30/10 7:58 AM

To: accountprotectteam2010 @ hotmail.com **Microsoft Live Account Alert!!!** Dear Account Owner This Email is from Microsoft Customer Care and we are sending it to every Hotmail Email User Accounts Owner for safety. we are having congestion's due to the anonymous registration of Hotmail accounts so we are shutting down some Hotmail accounts and your account was among those to be deleted. Please verify your account and let us know if you still want to use this account. If you are still interested please confirm your account by filling the space below. Your User name, password, date of birth and your country information would be needed to verify your account.

- Username: .....
- Password: .....
- Date of Birth: .....
- Country or Territory: .....

Confirm you're E-mail by filling out your Login Information below after clicking the reply button, or your account will be suspended within 48 hours for security reasons. Sincerely,
The Windows Live Hotmail Team

(b) **Pharming**

Pharming occurs when a hacker redirects website traffic from a legitimate website to the hacker's fraudulent website by exploiting vulnerabilities in the Domain Name System (DNS). By corrupting a computer's knowledge of how a site's domain name maps to its IP address, the attacker causes the victim's computer to communicate with the wrong server—a technique known as domain hijacking.

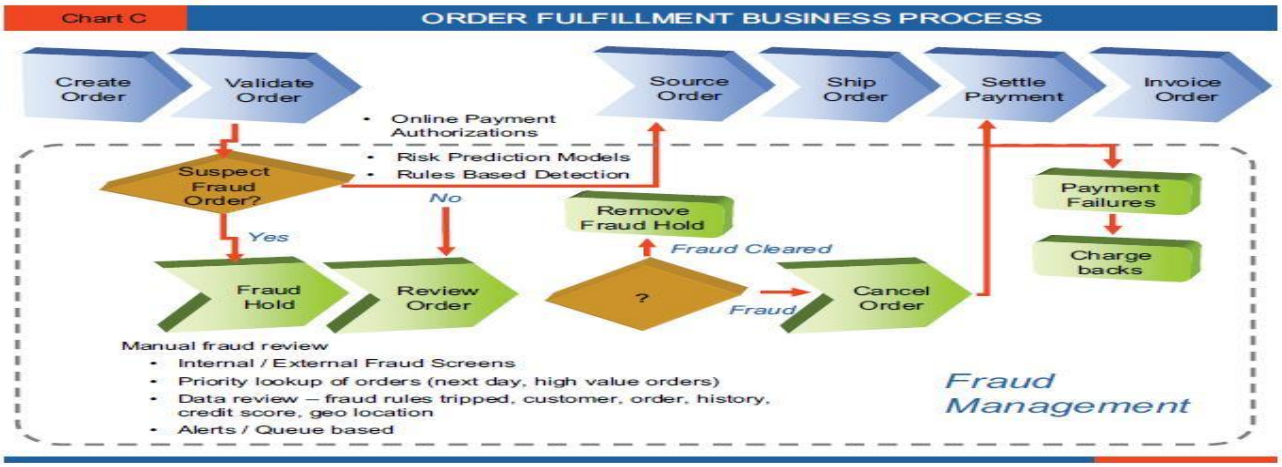
By constructing a fake web site that looks like a legitimate site that might ask for the user's personal information, such as a copy of a bank's website, the fraudster can "phish", or steal by means of false pretenses, a victim's passwords, PIN or bank account number. The combination of domain hijacking with a phishing website constitutes farming.

Although many such sites use the Secure Sockets Layer (SSL) protocol to identify themselves cryptographically and prevent such fraud, SSL offers no protection if users ignore their web browsers' warnings about invalid SSL server certificates. Such warnings occur when a user connects to a server whose SSL certificate does not match the address of the server.

VI. DEFENDING THE FAITH IN VIRTUAL WORLD:

Web has become the prominent part of our life so we need a complete protection which can retain our faith. As we have been facing a problem of cyber laws in India which has no relevant result. Cyber act 2005 does not protect the users from fraud because there is no solution of virtual world crime in real world so we need some virtual guards who can catch them in their world. Infosys is working on this concept very passionately since they have introduced the system on line fraud

management system. Almost 28% of all online orders are affected by fraud. The efficiency of the fraud management process thus has a direct impact on ecommerce profitability, operating efficiency and scalability.



VII. CONCLUSION:

Easy money always been a razzmatazz, everyone wants to be around it. People those who get buzzed around it in initial stage get benefited and finally the easy money maker get benefited. The ponzi schemes are luring the people since it came in existence and people are being cheated too. It's totally illogical to make money from ponzi schemes for investors. Only three levels are possible[6] after that only company can make out money from so called Ponzi schemes. One thing is having a high level of paradox in this issue and that is, internet literate people are the victim of these fraud so only awareness is not a sufficient solution. A real but virtual guardian is required to shield investor from the great internet fraud factories. Ethics are conventional but cyber ethics has to be implemented with all its new definitions and code of conducts. Notions are changed but the rate of change measured high in virtual world. Now we are in a situation where we are supposed to start an ethical debate on cyber ethics from scratch.

REFERENCES:

[1] Remarks by Alan Greenspan former fedral reserve chairman on CNBC, July 16, 2002, quoted by Patricia Aburdene in Megatrends 2010: The Rise of Conscious Capitalism .
[2] Infosys white paper on "Fraud Management in the online retail environment" by G.S Paintal ,www.infosys.com
[3] http://www.scambusters.org/onlinesurveys.html ,Internet ScamBusters™ The #1 Publication on Internet Fraud By Audri and Jim Lanford Issue #150)
[4] httpwww.indianexpress.comnewsspeak-asia-fraud-rs-2-000-crore825777
[5] http://www.suchetadalal.com/?id=a60a3ffc-a8bd-0368-492e822e450e&base=sub_sections_content&f&t=Home+Trade%27s+%27starry%27+gameplan
[6] described in pyramid table mentioned above.
[7] http://en.wikipedia.org/w/index.php?title=Internet_fraud&action=edit&section=26