December 2006

Negotiation and Power in the Cybercrime Framework

Chad Albrecht
Institute for Labor Studies- ESADE Business School

Conan Albrecht
Marriott School of Management- Brigham Young University

Jonathan Wareham
ESADE Business School

Paul Fox
ESADE Business School

Negotiation and Power in the Cybercrime Framework

Chad O. Albrecht
Institute for Labor Studies
ESADE Business School
Chad.Albrecht@esade.edu

Conan C. Albrecht
Marriott School of Management
Brigham Young University
conan@warp.byu.edu

Jonathan Wareham
ESADE Business School
Jonathan.Wareham@esade.edu

Paul Fox
ESADE Business School
Paul.Fox@esade.edu

ABSTRACT

Given the growing prevalence of Internet fraud and its enormous social costs, the goal of this article is to advance theoretical understanding of the power that perpetrators use when influencing victims in fraudulent transactions. Specifically, the article proposes an interactive model, combining the dimensions of power and negotiation from the management and psychology literature. We then examine the moderating effects of the Internet on the communication and fraud process between perpetrator and victim, as well as some of the major tactics employed to appeal to each power type in predominant fraud forms.

KEYWORDS

Internet, Fraud, Cybercrime, Power, Negotiation, Deception

INTRODUCTION

Over the last several decades, the subject of fraud has received substantial attention in nearly all fields of management. Frauds such as Enron, WorldCom, Tyco, and Adelphia have resulted in a mistrust of the United States accounting standards and profession, causing the accounting rule makers and government regulators to reevaluate and reestablish basic accounting procedures (Apostolon and Crumbley, 2005). Large frauds around the world such as Parmalat, Harris Scarfe, HIH, and Allied Irish Bank show that these disasters are not just occurring in the United States, but are prevalent throughout the world. One conservative estimate suggests that organizations in the United States lose more than six percent of their total revenue as a result of fraud (Association of Certified Fraud Examiners, 2004).

As described above, fraud has a large impact on society. However, in the last few years, as a result of technology and the explosive growth of the Internet, especially that of e-commerce, Internet fraud has become a major concern for consumers, merchants, and governments (Balsmeier et. al., 2005, National White Collar Crime Center et al. 2004). Gartner estimates that growth in electronic commerce and online financial services during the next three years alone will be one to three percentage points lower than if people were better protected online; and in the 12 months prior to May, 2005, within the United States alone, 2.4 million people lost $929 million to Internet fraud (Richmond, 2005). Many of these on-line consumer frauds are aimed at the uneducated, unaware, elderly, or immigrants, preying upon the most weak and susceptible of society (Lecovich, 2005; Marlowe and Atiles, 2005). In the past, committing fraud was more difficult and resulted in paper trails and other physical evidence. However, today a perpetrator can steal, conceal, and transfer assets with only the click of a mouse.

Almost daily, new frauds and scams arise using the Internet and other technological advances as the tools to perpetrate the crimes. Individuals throughout the world are approached, in many different ways, with fraudulent business deals, false money transfers, and other misleading exchanges in chat rooms, by email, on Internet pop-ups, or during Internet auctions. It has been suggested that 3 main areas of fraud exist on the Internet: securities law violations, crime and fraud in electronic commerce, and deceitful acts by Internet companies or individuals (Baker, 2002).

Internet fraud perpetrators exert considerable effort in order to influence and gain power over their faceless victims. An individual in a Internet chat room who claims to have private information about a public company, citizens of Nigeria who claim to have access to substantial funds, or illegitimate companies who con consumers into providing personal financial information are all examples of perpetrators' attempts to gain power over unwary victims.

Given the enormous costs of fraud and the growing prevalence of Internet fraud, the goal of this research is to advance theoretical understanding of the power that perpetrators use when influencing victims across the Internet. Specifically, the research proposes an interactive model combining the dimensions of power and negotiation from the management and psychological literature and applying it to the fraud process. The article then goes on to explain the role of the Internet and other technological advances on fraud using this model.

DEFINITION OF FRAUD

It has been suggested that there are two primary methods used to get something from others illegally: physical force and deception (Albrecht, et. al., 2006). Fraud is defined as:

A generic term, and embraces all the multifarious means which human ingenuity can devise, which are resorted to by one individual, to get an advantage over another by false representation. No definite and invariable rule can be laid down as a general proposition in defining fraud, as it includes surprise, trickery, cunning and unfair ways by which another is cheated. The only boundaries defining it are those, which limit human knavery (Webster's New World Dictionary, 1964).

DEFINITION OF NEGOTIATION

Negotiation has been defined as "an interpersonal decision-making process by which two or more people agree how to allocate scarce resources" (Thompson, 2000). Both researchers and practitioners have spent much time and resources to better understanding the negotiation process (Lewicki, et. al., 1999) and its' various influences, including the negotiators' bargaining history and its' effects on future negotiation performance (O'conner et. al., 2005). When a fraud takes place, the fraudulent transaction can be described as a negotiation. In the fraud setting, the perpetrator and victim make an interpersonal decision to allocate resources, with the victim transferring resources to the perpetrator (often for some promised return or false representation). When the fraud takes place, from both the perpetrators and the victims' perspectives, a successful negotiation has taken place. It usually isn't until some time later that the victim learns that he or she has been deceived into a fraudulent negotiation.

Proposition 1: When a fraud takes place, the perpetrator and the victim both believe they have participated in a successful negotiation.

DEFINITION OF POWER

Since the process of negotiation and its effect on individuals and transactions was first introduced into the psychology literature, one of the fundamental variables that has been studied has been that of power (Marwell et al., 1969). Power is a critical factor and fundamental element for success in the negotiation process (Kim et. al., 2005). Weber (1947) introduced power as the probability that a person can carry out his or her own will despite resistance. When a fraud takes place, the perpetrator has the desire to carry out his or her will – taking advantage of the victim through deceit – regardless of resistance. Most of the power literature since Weber's time has supported his basic definition (Bacharach & Lawler, 1980). In order to understand power, French and Raven (1959) introduced a framework that has, arguably, become the most commonly referenced appraisal with regards to power in the management literature (Kim et. al, 2005).

Proposition 2: Understanding the relationship between power and negotiation in the fraud process can help researchers and practitioners understand, research, and evaluate fraudulent transactions more fully.

French and Raven (1959) propose that power is comprised of five separate variables, each stemming from the different aspects of the relationship between the actor and the actor's target of influence. It has been said that these 5 power bases have stood the test of time (Dapiran and Hogarth-Scott, 2003). Specifically, French and Raven suggest that A's power over B is determined by (1) A's ability to provide benefits to B (reward power), (2) A's ability to punish B if B does not comply with A's wishes (coercive power), (3) A's possession of special knowledge or expertise (expert power), (4) A's legitimate right to prescribe behavior for B (legitimate power), and (5) the extent to which B identifies with A (referent power). Using these five definitions it is possible to divide power into various categories and create five subtypes of power. Figure 1 presents the five types of power.

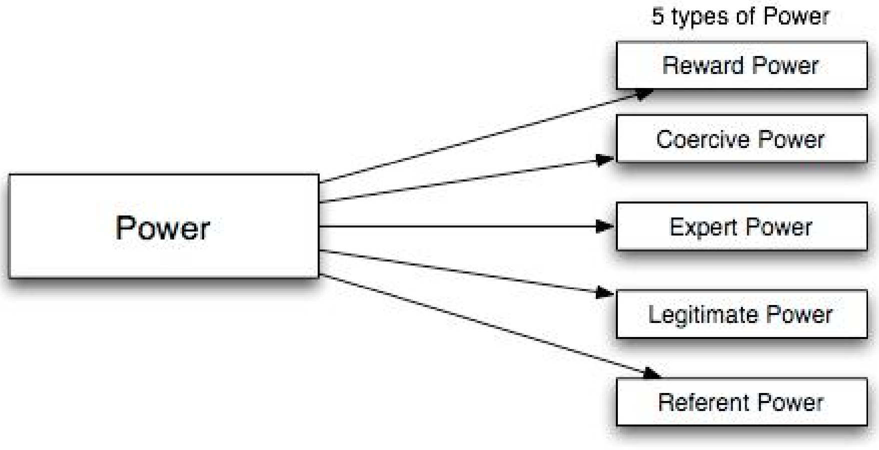

Figure 1: Five Types of Power

This model explains the types of power that are used in the relationship between the actor and the actor's target of influence. However, recent research on these types of power in the negotiations process has shown that it is perceived power, rather than actual power, that affects the outcome of any given negotiation (Wolfe and McGinn, 2005). Even if A doesn't actually have power over B, if B perceives A to have power, then it is as if A truly has power in the negotiation process. Hence these five types of power can be classified as perceived reward power, perceived coercive power, perceived expert power, perceived legitimate power, and perceived referent power. In this paper, we introduce the idea that, applied to fraud, perceived power is used as a means to influence the negotiation between the perpetrator and the victim. As can be seen above, the perpetrator must deceive the victim into negotiating using one of the five types of perceived power.

Proposition 3: To fully comprehend the role of power in fraudulent transactions, it is necessary to interpret the five different types of power as perceived power.

Perceived reward power is the ability of the perpetrator to convince the victim that he or she will provide the desired benefits through a negotiation. The promise of a monetary reward for participation in a Nigerian money scam, the promise of validation of personal information in a phishing operation, or the promise of high-paying jobs as a bogus mystery shopper are all examples of reward power.

Perceived coercive power is the ability of the perpetrator to make the victim perceive potential punishment if he or she doesn't participate in the negotiation. This potential punishment is usually based on fear (Politis, 2005). If the victim perceives that the perpetrator has the ability to punish him or her in any way the perpetrator begins to exercise a form of coercive power over that individual. Perceived coercive power is a tool often used by CEOs, CFOs, and other executives when a financial statement fraud takes place. Executives will often use coercive power to influence employees and others to participate in the fraud. These individuals fear they may lose their jobs, or be discriminated if they do not participate. Perpetrators can use coercive power, via the Internet, in at least four ways (1) by gaining personal information about the victim through spoofing, sniffing, or data theft, (2) through processes such as click through frauds or other physical fraudulent means, (3) deceiving the victim to believe that the perpetrator can do physical harm to them, and (4) persuading the victim that if they do not act now the opportunity will be lost.

Perceived expert power is the ability of the perpetrator to use influence through means of expertise or knowledge. Examples of frauds that involve perceived expert power include perpetrators who claim to have access to non-public or other sensitive information or perpetrators who claim to have a special knowledge of a given activity. Deceiving a victim into believing that a perpetrator has expert knowledge or expertise is using expert power to influence a victim. In one of the most well known frauds of all time, Charles Ponzi conned victims into believing that he had expert knowledge in foreign postal coupons. Charles Ponzi claimed that he could make significant profit for investors by purchasing stamps in Spain for about 1 cent (N.Y. Times, 1920) and selling them in America for six cents. Using this "expert knowledge" he deceived individuals out of millions of dollars and gave birth to the popular phrase "Ponzi Scheme."

Perceived legitimate power is the ability of a perpetrator to convince victims that he or she has some form of real power over them. Often, this type of fraud involves individuals claiming to represent the individual's church, community, or organization. The perpetrator assumes some form of authoritative role and convinces the victim that such authority is legitimate. An example of this type of fraud is the "Greater Ministries" fraud. Individuals were told to invest money into programs such as the "Double Your Money" program and the "Faith Promises Program." Members of the congregation were promised that they would double their money in just 17 months. The fraud involved over 18,000 individuals who lost more than $448 million. In 2001, five leaders of the Greater Ministries International Church were convicted in federal court on a total of 72 counts of conspiracy, wire and mail fraud, and money laundering (Gibelman and Gelman, 2003).

Perceived reference power is the ability of the perpetrator to relate to the target of influence. Perpetrators will build relationships of confidence with a victim via an Internet chat room or other media. Perpetrators often use perceived reference power to gain confidence from victims and deceive them into fraud. Perceived reference power is possible because perpetrators characteristics, unlike other criminals, are very similar to the general population's characteristics (Romney, 1980). When fraud does occur, one of the most common reactions by those around the fraud is denial. Victims can't believe that he or she, a trusted friend, would deceive them and behave dishonestly (Albrecht, 2006).

DECEPTION

There are many cases where deception has been used in the negotiation process (Schweitzer, 1997). Not only is deception a part of many negotiations, but it has also been suggested that deception increases as the incentives for performance increase (Tenbrunsal, 1998). Deceitful negotiation has been used to fraudulently manipulate individuals throughout history. In the negotiation process it is deception that allows the perpetrator to falsely exercise power over the victim. The theory of deception identifies seven operational tactics employed to deceive a victim (Grazioli and Jarvenpaa 2003b; Johnson et al. 2001). As a primarily tactical model, it compliments our model of power types, suggesting the specific mechanisms that the con artist may employ to realize specific power forms over the victim.

Available Tactics in the Theory of Deception-

from (Grazioli and Jarvenpaa 2003b)

Tactic	Definition
Masking	Hiding or destroying critical information
Dazzling	Disguising critical information
Decoying	Distracting the victim's attention away from critical information.
Mimicking	Assuming someone else's identity, or impersonating someone else.
Inventing	Making up information.
Relabeling	Presenting information in a misleading way.
Double play	Suggesting to victim that the victim is taking advantage of the deceiver.

Table 1: Available Tactics in the Theory of Deception

For example, research suggests that con-artists pretending to be businesses prefer masking, and relabeling, thereby achieving expert and legitimate power (Grazioli and Jarvenpaa, 2003a). Specifically focused on the Internet, Grazioli and Jarvenpaa (2000) studied the effectiveness of dazzling, inventing, and relabeling for disguising fraudulent web sites, often used to achieve reward, expert and referent power.

POWER AND DECEPTION ON THE INTERNET

Along with the developments in the Internet, opportunities to commit fraud and unethical acts have become more available. The Internet has created opportunities to exert perceived power and negotiation skills that were unheard of 20 years ago. And as technology continues to advance, perpetrators find new means and ways to deceive individuals and commit fraud.

Proposition 4: The Internet has become a significant, new instrument in the negotiation process between perpetrators and victims.

According to U.S. Federal Bureau of Investigation statistics (2004), the majority of perpetrators of Internet fraud make contact with the victim through e-mail (63.5%) or a webpage (23.5%). Internet auction fraud was by far the most common

(71.2%), but in terms of the size of the losses, check fraud ($3,600), Nigerian letter fraud ($3,000), and confidence fraud ($1,000) were the largest.

It has been suggested that fraud like other crime, can best be explained by three distinct factors: (1) a supply of motivated offenders, (2) the availability of suitable targets, and (3) the absence of capable guardians (Cohen and Felson, 1979; Krambia-Kapardis, 2001).

First, the Internet supplies a gathering place for an endless supply of offenders. The connectivity and global reach provided by the Internet means that these offenders can be anywhere in the world and through the Internet can communicate with anyone. Communication through email, the primary method of contacting victims, is instantaneous and practically free due to low transaction costs. The Internet also allows offenders the ability to easily customize their scams to individual users and the flexibility to quickly change the scam once it is discovered. In auctions alone, Chua and Wareham (2004) identified 11 different types of fraud, and state that "con artists know that developing specialized fraud schemes increases their profits while minimizing their risk of capture" (p. 33).

Second, the Internet supplies numerous suitable targets. Victims can be approached through e-mail, chat rooms, pop-up adds, websites and numerous other media via the Internet. Web sites like eBay, with its 181 million registered users worldwide, provide offenders with easy access to a large number of potential victims. However, access to potential victims is not exclusive to the Internet. Perpetrators of fraud can obtain personal information in a number of ways, including: stealing wallets, purses or credit cards; stealing mail or through sending a fraudulent address change form; through viruses or spyware; or through unsolicited emails or telephone calls, and in over half the cases the offender has a prior relationship with the victim (Diller-Haas, 2004).

Third, the Internet provides a perfect scenario for fraudulent activity with few or no capable guardians. The Internet has no boundaries; it crosses communities, cultures, and countries. Much fraud crosses national and international legal jurisdictions, and, hence, perpetrators have little risk of getting caught or punished. For example, while many states within the United States have statutes relating to Cybercrime such as money laundering, identity theft, online gambling, and cyber stalking, there is no standard and the rules vary from state to state (Brenner, 2001). Because most of these statutes were written before the Internet existed, the statutes only relate to property, computer, or other types of illegal acts and do not specifically address Cybercrime. Fraud is a covert crime, making collection of evidence for prosecution difficult; it is nonviolent so it receives less evidence by society and lower priority by law enforcement; most Internet frauds are small and thus victims have little incentive to prosecute; and when offenders are caught they often receive light sentences (Chua and Wareham, 2004).

Proposition 5: Fraud is becoming more widespread because the Internet supplies a gathering place for an endless supply of offenders, offers numerous suitable targets, and provides a scenario for fraudulent activity with few or no capable guardians.

A COMPREHENSIVE MODEL

To understand the interaction between power, negotiation, and the Internet, the following model is presented. On the left are French and Raven's five types of power. The offender will use the five types of power to deceive the victim into the negotiation. The middle box represents deception, which is enhanced through technological advances, such as the Internet, electronic commerce, or any other technological media used for communication. The right hand box represents the victim, including the victim's emotions that the perpetrator will try to manipulate and use in the deception process. The successful negotiation is the final outcome of the perpetrator using power to deceive via the Internet the victim by manipulating the victim's emotions.

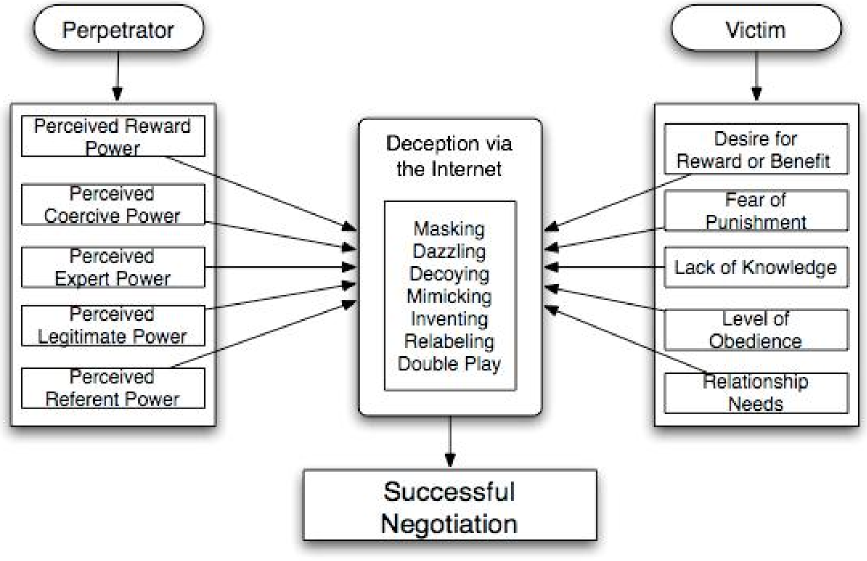

Figure 2: The Cybercrime Framework

In all scams, there is some perceived reward that is never fully realized, or is misrepresented in some way, whether in the form of money, which never arrives, or goods or services, which are not provided or are somehow less than that which was promised. The key to whether the negotiation is successful or not hinges on the perception on the part of the victim as to the size of the reward as well as the victim's perception that the offender is legitimate. The perceived expert power has a positive relationship with perceived legitimate power. Furthermore, the perceived referent power is increased through repeated interactions between offender and victim, and also has a positive relationship with perceived legitimate power. Coercive power is generally used to create the impression that the offer is unique and for a limited time, and can create a sense of urgency in the negotiation.

To illustrate this model, we present the top ten Internet scams of 2005 in Table 2 (Internet Fraud Watch, 2005). In the table, we posit how each type of fraud appeals to a specific type of power, as well as the predominant deceit tactics employed to exercise each power.

Perpetrator	**Perceived Reward Power**	**Perceived Coercive Power**	**Perceived Expert Power**	**Perceived Legitimate Power**	**Perceived Referent Power**
Victim	**Desire for a Reward or Benefit**	**Fear of Punishment**	**Desire for a Need or Want**	**Level of Obedience**	**Relationship Needs**
Deception via the Internet	Dazzling Decoying Mimicking Inventing Relabeling	Mimicking Inventing Double play	Decoying Dazzling Mimicking Relabeling	Decoying Mimicking Relabeling Double play	Dazzling Mimicking Inventing Double play
Auctions	Seller misrepresents product; Shilling/collusion	Auction fever-buyers must act before	Seller may pose as expert in antiques or	Reputation scores – can be inflated by	Trust relationship created through

	artificially increases price	auction close	one-of-a-kind merchandise. Cut and paste from real experts	seller Seller poses as reputable company	community forums
General Merchandise	Seller misrepresents product		Seller may pose as expert in antiques or one-of-a-kind merchandise. Cut and paste from real experts	Seller poses as reputable company	Seller creates trust through interactions with buyer
Nigerian Money Offers	Promise of large financial rewards	Offer is confidential and for a limited time		Offender poses as high government official – gives evidence of legitimacy	Appeals to needs of under-developed regions
Fake Checks	Victim perceives that checks are valid			Victim perceives that offender represents a legitimate company	Offender creates trust relationship through interactions with victim
Lotteries	Promise of large financial rewards	Offer is for a limited time		Offender poses as a reputable institution	
Phishing	Victim expects validation of personal information	Offender argues that user data has been stolen hence possible injury – updates required		Offender poses as a reputable institution known to the victim	
Advance Fee Loans	Victim is promised loan in spite of his/her bad credit			Offender poses as a reputable institution	
Information/Adult Services	Victim receives expected services but with hidden			Offender poses as a legitimate	

	conditions			institution	
Work-at-Home	Promise of large financial rewards		Offender poses as expert in home businesses	Offender poses as a reputable institution	
Internet Access Services	Cost of services misrepresented or services not provided			Offender poses as a reputable institution	

Table 2: Internet Crime within the Cybercrime Framework

The perceived reward in auctions can be manipulated through various means. The seller can engage in shilling or bid shielding, where the price of the goods is artificially driven up through some behavior on the part of the seller. This creates the impression that the goods are more in demand than they actually are, resulting in higher bids from “legitimate” buyers. The goods can also be misrepresented, where the seller describes an item incorrectly and thus the actual reward is less than what is perceived. Auctions also have a coercive nature, where the buyers feel that they must act immediately or lose a unique opportunity.

Perceived expert power can be exercised in auctions, for example, in the case of goods which are supposedly antiques or one-of-a-kind, and the seller poses as a knowledgeable collector.

Perceived legitimate power can be created through the reputation scores which maintained on auction sites based on the number of situations where the buyer is satisfied or dissatisfied. These scores can be manipulated, however, through “phantom” trades where the seller poses as a buyer on various trades and gives himself positive ratings, thus artificially elevating his reputation score.

Finally, perceived referent power can be obtained through the reputation scores as well as other community forums on the auction sites, where buyers and sellers can interact and perpetrators can gain the confidence of their potential victims.

For each power form, we explore how the Internet enables specific tactics like mimicking, inventing, and relabling relatively easy to execute. The increased anonymity, global reach and low barriers to entry enable fraudulent activity from all parts of the world.

FUTURE RESEARCH

Our model identifies five types of power, the primary tactics utilized to realize the power, and the common fraud types where these elements are manifest. The next step in this research is rigorous empirical validation with both aggregate data analysis as well as controlled experimentation. Understanding the ways in which perpetrators of fraud are able to exert these five types of power across the Internet is a first step towards helping regulators, companies and individuals develop better strategies for its control and prevention.

CONCLUSION

Our purpose is to advance theoretical understanding of the specific power forms that perpetrators use when influencing victims in fraudulent transactions. Our model combines the dimensions of power and negotiation from the management and psychological literature as well as Internet fraud research from the Information Systems field. We then examine the moderating effects of the Internet on the communication and fraud process between perpetrator and victim, as well as deception tactics employed to realize each power type in frequently occurring fraud forms.

ACKNOWLEDGEMENTS

The authors would like to thank the Generalitat de Catalunya (Government of Catalonia) for financially supporting this research.

REFERENCES

1. Albrecht, W. S., Albrecht, C. C., Albrecht, C. O., *Fraud Examination 2nd Edition*, 2006. Thomson South-Western, United States of America.

2. Apostolon, N., and Crumbley, D. L., 2005. Fraud Surveys: Lessons for forensic Accounting. *Journal of Forensic Accounting.* Volume IV. Pp. 103-118.

3. Association of Certified Fraud Examiners. 2004 *The Report to the Nation on Occupational Fraud and Abuse,* (ACFE, Austin, Texas).

4. Bacharach, S. B., & Lawler, E.J. 1980. *Power and politics in organizations*. San Francisco: Jossey-Bass.

5. Baker. C. R. 2002, Crime, fraud and deceit on the Internet: Is there hyperreality in cyberspace? Critical perspectives in accounting? 13:1 pp. 1-15

6. Balsmeier, P., Blaise, J. B., Viosca, R. C. Jr., 2004. Internet fraud: A global perspective. *Journal of E-Business*, Volume 4: 1.

7. Brenner, S. W., 2001. State cybercrime legislation in the United States of America; a survey. *Richmond Journal of Law and Technology*. Volume: VI: 3.

8. Chua, C.E. and Wareham, J. 2004. Fighting Internet auction fraud: an assessment and proposal. *IEEE Computer*. .Vol.37, Iss. 10; pg. 31

9. Cohen, L. and Felson, M. 1979. Social change and crime rate trends: A routine activity approach, *American Sociological Review*, vol. 44, pp. 588-608.

10. Dapiran, P. G., Hogarth-Scott, S., 2003. Are co-operation and trust being confused with power? An analysis of food retailing in Australia and the UK. *International Journal of Retail & Distribution Management*, Volume 31: 5, pp. 256-267.

11. Diller-Haas, A. 2004. Identity Theft: It Can Happen to You. *The CPA Journal;* Apr 2004; 74, 4; p. 42

12. French, J. R. P., Jr., & Raven, B. 1959. The bases of social power. In D. Cartwright (Ed.), *Studies in social power:* 150-167. Ann Arbor: University of Michigan Press.

13. Gibelman, M., & Gelman, G. R., 2003. Should we have faith in faith-based social services? Rhetorical verses realistic expectations, *Nonprofit Management and Leadership*. Volume 13: 1, Pages 49-65.

14. Grazioli, S., and Jarvenpaa, S.L. (2000) "Perils of Internet Fraud: An Empirical Investigation of Deception and Trust with Experienced Internet Consumers," *IEEE Transactions on Systems, Man, and Cybernetics- Part A: Systems and Humans* (20:4), July 2000, pp 395-410.

15. Grazioli, S., and Jarvenpaa, S.L. (2003a) "Consumer and Business Deception on the Internet:Content Analysis of Documentary Evidence," *International Journal of Electronic Commerce* (7:4) 2003a, pp 93-118.

16. Grazioli, S., and Jarvenpaa, S.L. (2003b) "Deceived: Under Target Online," *Communications of the ACM* (46:12), December 2003, pp 196-205.

17. Internet Fraud Watch/National Fraud Information Center. 2005. Internet Fraud Statistics. January through December, 2005. Available at http://www.fraud.org/2005_Internet_Fraud_Report.pd

18. Johnson, P.E., Grazioli, S., Jamal, K., and Berryman, R.G. (2001)"Detecting Deception: Adversarial Problem Solving in a Low Base-Rate World," *Cognitive Science* (25:3), May/June 2001, pp 355-392.

19. Kim, P. H., Pinkley, R. L., Fragale, A. R., Power dynamics in organizations, *The Academy of Management Review*: 30:4, 2005. Pp 799-822.

20. Krambia-Kapardis, M. 2001. *Enhancing the auditor's fraud detection ability: An interdisciplinary approach*, Peter Lang, Frankfurt am Main.

21. Lewicki, R. J., Saunders, D. M., & Minton, J. W. 1999 *Negotiation* (3rd edition) Boston: Irwin-Mcgraw Hill.

22. Locovich, E., 2005. Elder abuse and neglect in Israel: A comparison between the general elderly population and elderly new immigrants, *Family Relations*, Volume 54: 3.

23. Marlowe, J., Atiles, J. H., 2005. Consumer fraud and Latino immigrant consumers in the United States. *International Journal of Consumer Studies*, volume 29: 5.

24. Marwell, G., Ratcliff, K., Schmitt, D. R., 1969. Minimizing differences in a maximizing game. *J. Pers. Soc. Psychol.* 12: 158-163.

25. National White Collar Crime Center, and Federal Bureau of Investigation (2004) "IC3 2004 Internet Fraud Report: January 2004-December 2004," Washington, DC, 2004.

26. N.Y. Times. July 30, 1920. Al. 1, Column 7.

27. O'conner, K. M., Arnold, J. A., Burris, E. R,. 2005. Negotiators' bargaining histories and their effects on future negotiation performance, *Journal of Applied Psychology*, 90: (2)

28. Politis, J. D., 2005. The influence of managerial power and credibility on knowledge acquisition attributes. *Leadership & Organization Development Journal*. Volume 26: 3, pp. 197-214.

29. Richmond, R. 2005. Internet Scams, Breaches Drive Buyers Off the Web, Survey Finds. *Wall Street Journal,* (Eastern Edition). New York, N. Y. : Jun 23. 2005. Pg. B.3.

30. Romney, M. B., Albrecht, W. S., Cherrington, D. J., 1980. Red-flagging the white-collar criminal, *Management Accounting.* March, 1980. Pp. 51-57.

31. Schweitzer, M. E., 1997. Omission, friendship, and fraud: lies about material facts in negotiation. Presented at Annu. Meet. Acad. Manage., Boston, MA.

32. Tenbrunsel, A. E., 1998. Misrepresentation and expectations in an ethical dilemma: the role of incentives and temptation. *Academy of Management Journal*. 41: 330-339.

33. Thompson, L. 2000. The Mind and Heart of the Negotiation. Prentice-Hall. United States of America.

34. Thompson, L. 1990. An Examination of naïve and experiences negotiators. *Journal of Personality and Social Psychology*, 59: 82-90.

35. U. S. Department of Justice. 2000. Internet Fraud. May 8 [on-line]. Available HTTP: http://www.usdoj.gov/criminal/fraud/text/Internet.htm

36. U.S. Federal Bureau of Investigation. 2004. IC3 2004 Internet Fraud – Crime Report. Available http://www.ic3.gov/media/annualreports.aspx

37. *Webster's New World Dictionary,College Edition,* Cleveland and New York: World (1964), p. 380

38. Weber, M. 1947. *The theory of social and economic organization.* New York: Free Press.

39. Wolfe, R. J., Mcginn, K. L., 2005. Perceived relative power and its influence on negotiations. *Group Decision and Negotiation.* Volume 14: 1, pp. 3-20.