RESEARCH ARTICLE OPEN ACCESS

Internet Fraud Analysis

Azhar Ushmani
Cyber Security
Western Governor University
Salt Lake City, Utah
USA

ABSTRACT
The fraud on the Internet became a serious issue in the age of technology. Some areas of the usage of the World Wide Web have an especially high potential for the implementation of fraudulent practices. The securities sales and trade, for example, is one of these dangerous fields that become a concern for the US Securities and Exchange Commission (SEC) (Williams 1296). The electronic commerce also exposes a significant potential for misleading practices. The progress of this type of commerce parallels the raise of online fraud, which led to the development of preventive and punitive mechanisms that reduce the risk of application of the Internet fraud. Furthermore, the effective growth of the Internet-based enterprises resulted in the increase in fraudulent actions related to their activities. The e-commerce organizations can misuse online data themselves or become victims of such manipulations of the third party (Backer 98). All three of these areas of the Internet fraud – security manipulations, misuse of data in electronic commerce, and the manipulations around the Internet businesses – endanger safety of corporate and private participants and demand preventive measures.
Keywords:- Internet Security, Internet Fraud

I. SECURITIES FRAUD ON THE INTERNET

The development of digital technologies and the World Wide Web engendered the securities fraud on the Internet. Siegel and Worrall define this type of cheating as an intentional manipulation of "securities marketplace for profit" (367). The scholars differentiate between three major types of such frauds: market manipulation, "fraudulent offerings of securities," and illegal touting (Siegel & Worrall 367). The frauds of the first type describe the manipulation of stock prices on the Internet market by an entity or person who changes the natural flow of demand and supply. These crimes divide into the categories of "cyber smear" and "pump and dump" (Siegel and Worrall 367). The latter scheme involves an artificial inflation of the price in online descriptions, while the former downplays the real price of the stock. Both of these crimes include the placement of falsified data on the Internet with the aim to gain money by manipulating the stakeholders' actions.

The second type of the Internet securities fraud is based on a construction of specific websites. These portals are "specifically designed to sell securities fraudulently," as Siegel and Worrall (367). The creators of such websites promote their product through unrealistically high profits the stakeholders would receive. However, the product is actually non-existent and the investments go directly onto the criminals' account. In some of such schemes, earlier investors receive some returns taken from the subsequent contributors' expenditures. This "system usually collapses" at some point, when the later investors receive no returns (Siegel and Worrall 367). The illegal touting, on the other hand, is a placement of false information online about an already existing company. In such scheme, the perpetrators promote an enterprise's product under a payment from this business. The illegal part of this activity concerns their failure to disclose to the customers that their "securities recommendations" are pre-paid (Siegel and Worrall 367). These main types of the Internet securities fraud must be taken into account when conducting business activities online.

These online manipulations violate the securities laws of the United States. The Securities and Exchange Commission (SEC) is the organization responsible for prevention and regulation of the online securities fraud. SEC began operating in the early twentieth century and developed the Securities Exchange Act of 1934 (Williams 1235). With the raise of the Internet in the late nineties, the activity of the Securities and Exchange Commission expanded into the area of online fraud. This institution attempts to regulate

the legislation for Internet securities while covering the area of economic investors and social investors (Williams 1277). The regulations issued by SEC are the foundation of the legislation of the Internet security and the main tool of combating online fraud.

The Commission also provides information for private Internet users helpful to assess and avoid cyber security attacks. SEC created an online database, EDGAR, that makes all reports open for the public (Williams 1179). Such overt work of this organization fosters the awareness of the country residents on the issue of the cyber fraud on the Internet. This development is especially important because 90% of "national cyber infrastructure" is in private possession and, thus, cannot be corporately operated (Farwell 2). For this reason, citizens must maintain security of their personal data transmitted through the Interned themselves. The information provided by SEC aids the private Internet users to assess and prevent the Internet security manipulations.

II. FRAUD IN ELECTRONIC COMMERCE

The fraud in e-commerce engendered by the rapid growth of this type of business is another important area of online manipulations. Individual and corporate customers need protection to feel safe when participating in e-marketing. However, fraud prevention in electronic commerce is difficult because the electronically transmitted data can be easily accessed and manipulated. For this reason, various organizations created tools and strategies that reduce risks of fraudulent manipulation in e-commerce.

One way to fight fraud in electronic commerce is by making customers and stakeholders aware of the manipulations. Saenger et al. maintain that electronic marketplaces may be "manipulated by malicious sellers" who represent their reputation as higher than in reality (3870). The authors attempted to develop new technology to help the Internet users in determining fraud on e-commerce. Saenger et al. conducted an experiment with German and British users to compare their ability "to detect malicious behavior" by reading feedback on such sites as eBay and through a newer interactive interface (3870). The results favored the new interface that aided in detecting fraudulent behavior with higher efficiency. This study shows that the interactive interface is better suited for combatting the e-commerce manipulations.

Another possibility to fight fraud is by preventing the criminals from successful access of the private information. This method is especially important in such area as banking, where the financial institutions hold the data of private and corporate customers online, such making this information susceptible to cyber crime. Wright and Hu suggest a method of evaluating the safety of the transaction produced by different mathematical models (1). Through the application of specific "segmoidal functions," the authors estimate the risk of the implementation of different models (Wright and Hu 1). Such evaluation permits choosing for application and commercial usage only the mathematical codes that provide the highest data protection. This method should make the banking data much safer than before. These and other mechanisms protect customers and corporate participants engaged in e-commerce from fraudulent manipulations.

III. FRAUD DEPENDING ON THE INTERNET COMPANIES

The rapid growth of Internet companies led to the development of a specific field of online fraud. In the early new millennium, a number and the income of such companies suddenly increased and as decreased with the same speed (Backer 97). These web-based enterprises depend on their digital form and, therefore, are subject to cyber crime. Since the first surge of the Internet-based companies, practices of such fraud developed into a dangerous field of crime. The wide variety of aspects susceptible to online manipulations makes both the Internet businesses and their customers especially vulnerable. On the one hand, activities of some of such enterprises "border on fraud," according to Backer (97). On the other hand, many of the Internet businesses lose control over their data placed online due to the cyber theft and manipulation. Backer explains that this latter type of companies become victims of fraud because their environment, i.e. data placed online, is easily breached (97). The existence of different aspects of

the Internet businesses manipulation makes the creation of protective mechanisms difficult.

One of the areas of fraudulent information connected to the Internet companies is advertisement. Many online enterprises place ads for profit to make revenue. Backer maintains that for the majority of such companies, advertisement is the only source of income (98). These enterprises may be paid by the companies that place their ads on their pages according to the number of people who visit these sites. However, the amount of visitors is hard to measure because the individual "hits" do not necessarily correspond to the number of real persons but to the "number of links and graphic images" (Backer 98). Thus, the manipulation of this data becomes an area of fraud meant to increase the company's income from advertisements. The possible ways to prevent the Internet fraud in this field is to develop better strategies and tools in calculating the number of real hits (Backer 99). By providing the true information about the effectiveness of advertisement, these mechanisms will ensure the influence of the ad on the customers. Thus, the efficacy of the online placement will be correctly assessed and the fraud prevented.

Other types of fraud that endanger the Internet companies include the speculative stock promises. Some online-based enterprises virtually have no profits other than from the advertisement placed on their pages (Backer 98). However, due to the public interest in the new businesses these companies were able to gain a large number of stockholders. This development was especially active in the early new millennium due to the novelty of the Internet companies. Many of them advertised their income wrongly by publishing fake reports of financial analysts to attract stockholders (Backer 98). This data manipulation led to the inflated investors' interest in the Internet businesses and in the mass investment in this area of market. Consequentially, the "lack of economic substance" under the cover of the fraud resulted in the rapid decline of the market value of these enterprises (Backer 98). Thus, the cyber manipulation that caused the Internet companies' fast progress was also responsible for their subsequent fall.

These and other dangers of fraud in the area of Internet business require the attention of authorities to produce effective combatant strategies. SEC provides safety of online securities but does not take action in toward fraud related to the Internet enterprises (Backer 98). The potential threat of fraud related to the Internet businesses requires other organizations to take measures. Military offered several systems able to save users from those manipulations (Farwell 14-15). However, not all Internet-based businesses may be willing to disclose their information as required in cooperation with the US military. Farwell suggests the changes in the US legislation related to e-commerce and the Internet enterprises (17). The legislative reform may become the most effective measure in the fight of the electronic data manipulation related to the online-based businesses.

IV. CONCLUSION

The dangers of the Internet usage are great due to the variety of ways, in which the information placed online can be manipulated. These data is subject to security frauds that have several types of information misuse. The manipulation of data in electronic commerce is another important area of the Internet-related fraud. The deception on the side of the Internet businesses and the third parties is a source of concern for users, corporations and authorities. All these areas of online fraud demand new preventive measures, such as legislative reforms, effective data coding and fraud prevention strategies.

REFERENCE

[1] Backer, C. Richard. "Human and Social Perspectives in Information Technology: An Examination of Fraud on the Internet." *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications*, edited by Hamid Nemati. Information Science Reference, 2010, pp. 89-100.

[2] Farwell, James. "Industry's Vital Role in National Cyber Security." *Strategic Studies Quarterly*, vol. 6, no. 4 (2012): 10-41.

[3] Saenger, Johannes, et al. "Look before You Leap: Improving the User's Ability to Detect Fraud in Electronic Marketplaces." *CHI '16*, Proceedings of the 2016 CHI

Conference on Human Factors in Computing Systems, pp. 3870-3882.

[4] Siegel, Larry, and John Worrall. *Essentials of Criminal Justice*. Cengage, 2018.

[5] Williams, Cynthia. "The Securities and Exchange Commission and Corporate Social Transparency." *Harv. L. Rev.*, no. 112 (2018): 1197-1298.

[6] Wright, William, and Hung-Tzaw Hu. "Method and apparatus for evaluating fraud risk in an electronic commerce transaction." *U.S. Patents*, US Grant US7865427B2, 2011, pp. 1-10.