UDC 005.334:336.71
Review paper
Recived: March 03, 2021.
Acceptee: March 27, 2021.
Coresponding author: edingaraplija@fkn.unsa.ba

FRAUD - CONTEMPORARY CHALLENGES

Edin Garaplija

Institut za upravljanje rizicima i naučnoistraživački rad, ,doktorant Fakulteta za kriminalistiku, kriminologiju i sigurnosne studije, Sarajevo, Bosna i Hercegovina
edingaraplija@fkn.unsa.ba

Abstract: *The author's main attention is focused on the manifestations of fraud, which are the predominant ways of committing modern criminal activities in today's social and economic trends. The paper will first present a wide range of such illicit activities, which will be dichotomously classified into modernized classical forms and completely new types, most often in the predominantly online environment. Among other types of this type of criminal activity, the author especially emphasizes card fraud and identity theft, emphasizing such a high degree of damage they cause to damaging legal and natural persons. The author presents the trends of fraudulent activities according to the experiences of economically developed countries, whose economic systems are stable and whose standard of living is high. In addition to the theoretical and practical approach of experts in this field, the paper will list concrete examples of modern fraud as a kind of indicator of their presence and the degree of social danger, which determine them. The key intention of the author is to point out with this paper the necessity of changing the perception of citizens towards the seemingly harmless threats of these illegal activities, to which they are continuously exposed every day in a professional and private, primarily online, environment.*

Keywords: *Online fraud, internet environment, card fraud, identity theft, personal data.*

1. INTRODUCTION

Frauds are not new in the milieu of criminal activities because they are a faithful companion of the development of humanity. With the use of the Internet and the emergence of online environments in our private and public lives, as well as the global commercialization of the Internet, ways of misusing personal data for fraudulent activities have adapted to the online virtual reality environment [5].

Victims of such scams can be found easier and faster than targets outside the online environment. Undertaking electronic actions can be repeated in real time at high speed, so that internet scams can be directed multiple times to the same damaged party in a very short time. This is especially true for customers, who purchase online, which is why their personal data is exposed in online communication. In other words, modern forms of fraud involve any form of fraudulent activity consisting of one or more acts on the Internet for the purpose of committing a criminal offense [5].

Traditional methods of committing fraud have become more efficient and effective in relation to an unlimited number of potential victims, which has grown from individual cases of injured parties into a real market of possible targets of fraud [2]. Accordingly, the following are examples of the most common types of internet scams, which have evolved from their classic forms in the online environment. After that, we will consider the card fraud and identity theft as extremely frequent and harmful forms of modern fraud.

2. NEW MODES OF CLASSICAL CASES OF FRAUD

- Fraud by offering internet and online services

Free internet access is promised by purchasing software that is never provided. Consumers paid for the password to access the exhibited photos, but never received it, or were charged for the photo viewing program according to the amount of the international telephone call tariff. The producer paid for the location on the web to place ads for the sale of wine, but the ads were never published, which is why he was exposed to the cost of the price of the ad and the failed profit due to unrealized marketing activities. These are just some of the many examples of cases of classic forms of fraud, which are realized on a daily basis to the detriment of an immense number of individuals and legal entities in online circumstances.

- Supply of consumer goods

Selling by random or unsolicited e-mail, chatting, online discussion, one-time websites, online advertising of products for sale (from sports equipment to toys or everyday kitchen utensils), sale of items of importance to collectors (eg coats of arms of sports clubs, old books) , music albums, movies, etc.), where the ordered and paid goods never find their way to customers. These goods are never delivered or are delivered damaged, defective or inappropriate

- Online auctions

Offers via internet auctions on websites for the sale of antiques, new and used computer equipment, videos, computer games, etc. The sellers never delivered the items bought on the online sale or misrepresented their price. The offer of these products is fictitiously increasing, so that in reality there are fewer of them than deceived customers or they are not in stock at all. Often online sellers increase the prices of products, after they have announced the highest offers.

- Pyramid sales and multi-level marketing

The concept of pyramid sales is similar to multilevel marketing. Pyramid sales provide a financial incentive to hire new distributors. Such sales concepts are generally banned because it is in fact certain that financial pyramids are unsustainable due to the impossibility of constantly hiring new distributors. When this happens, most employees lose their invested money. The Internet offers opportunities to quickly establish multi-level marketing activities due to the rapid, if not simultaneous, availability of a large number of potential distributors.

- Business offers and fictitious franchise

In the online environment, investment in internet markets where the sale of goods or the offer of services is advertised is encouraged. The buyer can buy the so-called ATMs that will reportedly be rented immediately to the seller for the purpose of generating a profit. The potential profit from this concept of franchise is misrepresented or unfounded because the promised business offer is never realized, and the franchise does not exist.

- Engagement to work from home

These are false promises to engage in contact jobs to provide information or to approve credit card applications. One way of committing such scams is to sell computer equipment to an employee in order to create computer programs, which would allegedly be bought by the company that sold the equipment to the employee. The employee was allegedly deceived for the amount of computer equipment, which he paid to a non-existent company.

- Prizes and betting

In these cases, fraud is committed through a false promise that the payment of the registration fee will win a free trip, provided that the travel ticket is purchased at full price. The person who pays the registration fee and the cost of the travel ticket, allegedly wins a cash prize, but only after submitting the data on his bank account. The prize in the internet lottery can also be a discount on the price of a package

of satellite communication services with no payment of the main prize. In essence, in addition to not receiving a reward and paying non-existent registration fees and travel expenses, the deceived party also makes available funds in his bank account.

- Loan offers

Credit cards are offered on a number of websites or via spam, despite unfavorable creditworthiness, if the consumer pays an advance fee. Fee costs can be up to $ 100, and paid credit cards are never issued or delivered to the payer.

- Sales of manuals and guides for successful private life and business success

Fraud is committed to the detriment of the target group of Internet site users interested in ways of quick and easy earnings, improving the quality of psychophysical health, mastering unusual skills and acquiring special knowledge. After payment of the costs of advertised manuals, guides and similar publications, these printed materials are never delivered.

- Magazine subscription

By falsely advertising the provision of services for subscriptions to world-famous magazines, fraudulent payments of money are obtained for magazines that are never delivered to payers. If the payment is made from another continent, the readers' clubs are falsely displayed and the membership fee is charged so that the supposedly desired magazines can be bought at a lower price. These scams are often accompanied by other false information about discounts, where bank accounts are debited several times even though only one withdrawal of money has been approved.

- Computer 'hijacking'

The "hijacking" of a computer is, in fact, the taking over of some of its functions that communicate in the cyberspace of the Internet. First, the future deceived party, as bait, is offered a program for free viewing of images on a site. After downloading this program, the computer of the victim of fraud is disconnected from the network of the local Internet provider and connected to the site with images by dialing an international phone call. The time for which the deceived person views the images is the duration of the international telephone call, and the amount of the costs of this communication is paid to the perpetrator of the fraud.

3. CARD FRAUD

The totality of card frauds consists of abuses of debit, credit and other types of payment cards, which are performed for fraudulent purposes. In the UK alone, card fraud losses in 2019 amounted to 620,600,000 GPB [9]. At the same time, total spending realized through debit and credit cards reached the volume of GBP 829 billion in 2019, with an additional GBP 22 billion of the value of realized transactions [9]. Losses from card fraud will be presented in the following categories, which we determined according to the fact whether the card fraud was committed by distance purchase, counterfeit card, lost or stolen card, card that the user never received, as well as a card whose data was illegally downloaded or stolen. card identity.

- Card fraud committed by purchasing remotely or without displaying the card

This fraud occurs when a criminal uses illegally downloaded card data to make a purchase online, by phone or by mail. This type of fraud is mainly a consequence of the misuse of data that occurred through burglary of personal and card databases, "fishing" via e-mail and messages with manipulative content. The data obtained in the above ways are used for online shopping without the physical presentation of a payment card. Products are very often bought from geographically distant countries from the place of payment. Scammers also use social media profiles to advertise counterfeit discount sales to consumers. When a customer logs in to buy a product, a cybercriminal uses the stolen data from the customer's regular card and then withholds the amount the customer paid. Fake brokers are often advertised, who advertise goods and services at reduced prices, whereby these products are purchased by misusing data illegally downloaded from a valid card.

- Card fraud committed with a counterfeit card

This fraud occurs when the fraudster makes a fake card using the information obtained from the magnetic stripe of the used valid card. To obtain the information needed to create a counterfeit card, criminals typically place hidden or invisible devices through card readers at ATMs and uncontrolled payment terminals, such as self-service ticket machines at train stations, cinemas and parking lots. Counterfeit cards are usually used in foreign countries, where the pin and chip are not used in card making technology.

- Card fraud committed with a lost or stolen card

This fraud occurs when the holder of a criminal activity uses a lost or stolen card for purchase or payment remotely or directly, but also when he takes money from an ATM or in a bank. To commit this type of fraud, criminals use tactics, including stealing by diverting attention and capturing cards at ATMs. To get a card pin number, fraudsters usually look over the user's shoulder while using their cards in stores and at ATMs. Criminals also use small cameras, placed on ATMs so that they are aimed at the keyboard through which pin numbers are typed. In some cases, the victim is deceived into helping with a police investigation to hand over his card to a fake inspector or tell him his pin number.

- Card fraud committed with a card that the user has never received

This type of fraud occurs when a card is stolen in transit, after the card issuer sends it and before it is received by the original cardholder. Criminals typically target property with common zip codes, such as apartments and dormitories, or external mailboxes to commit such fraud. People who redirect mail after a change of address are also exposed to variations of this fraud.

- Card fraud committed by theft of card data ie card identity

The perpetrator of this fraud misuses the fraudulently obtained card or card data, as well as the personal data of the regular user, in order to open a new or illegally take over the existing bank account of the injured party. This type of fraud has two possible modes because it can be done by misusing other people's documents and illegally taking over accounts. In the first case, criminals use stolen or fake documents to open an account using fictitious or real personal data. For the purpose of their false representation, fraudsters usually steal documents, such as utility bills and bank statements, in order to obtain existing personal data which they will then use to commit fraud. Criminals can also use forged documents. Another variant of this type of fraud involves taking over an account by fraudulently using another person's credit or debit card account. The fraudster will first collect information about the targeted victim, then contact the card issuer (eg the bank) by falsely posing as the actual owner of the card, in order to be able to exploit the victim's bank account in the end.

4. IDENTITY THEFT

Much of the criminal activity in the online environment is aimed at identity theft, which is part of fraud with the misuse of someone's identity, which especially refers to the theft of personal data and their misuse and differs from the use of com-

pletely fictitious identity that can occur a combination of real or completely false data. Cyber fraudsters are intensively downloading and using personal data of living and deceased persons without authorization. Identity theft is a broad category that includes telephone or electronic contact in connection with alleged theft of a wallet or mail, impersonation on the Internet, or other fraudulent activity to obtain the personal information of a potential victim of future fraud.

Although it seems difficult at first glance, in practice it is very easy to get other people's personal data. All you need is a phone call, direct contact or sending an e-mail, with the demonstration of a fake profile of a bank representative, telephone or internet provider or "competent" state authority in order to submit a request for someone's personal data. After the established contact with the targeted victim, the reason for contacting is mostly false problems with the internet connection or user's computer, which is why as part of solving these difficulties the necessity of finding out information about card or bank data is stated. [1].

Identity thieves are not only disrupting the standard of living of victims by devastating bank accounts, unauthorized credit card payments, and reducing creditworthiness due to over-indebtedness. These cybercriminals also often deceive government agencies and taxpayers by using stolen personal data to file fraudulent health care bills to collect insurance or by claiming privileged social security status, to which they are not legally entitled. Online criminals also use illegally taken social security numbers to commit tax fraud or fictitiously apply for employment in order to receive unauthorized compensation for a non-existent, and thus unrealized, work schedule.

The growing use of commercial tax filing software and online tax filing services has led to the possibility for criminals to commit fraud without first stealing social security numbers [3]. In some cases, illegal access to an existing customer account is achieved by simply entering his username or e-mail address with software guessing the appropriate password. This is often referred to as taking over an account after identity theft and does not necessarily refer to the main bank account, but mostly to smaller funds stored on card accounts.

Whether the online fraudster uses this method to access an existing account or uses stolen personal information to create a new account, the end result is often the same because as early as the tax filing deadline, the fraudster files a false tax return using the victim's identity email or your bank account. The victim discovers this theft only when he submits a request for a refund, and the competent tax authority refuses to accept it, explaining that the refund has already been realized.

The theft of the health insurer's identity occurs when someone, in addition to the generals of the individual and his social insurance number, illegally takes over the victim's health insurance number in order to provide medical care, obtain prescription drugs or hand over fictitious treatment bills to the detriment of health insurance. This type of identity theft can endanger someone's life and health, damage a credit rating and endanger the health insurance of a large number of taxpayers [3] .

As an example of identity theft, caused by a previous burglary of personal databases, we cite the case of "Equifax" from 2017, during which cyber criminals obtained private data of more than 145,000,000 people, which makes almost half of the population of the United States [4]. The fraudsters broke into personal databases through automatic telephone calls, presented by 'Equifax', in order to verify the data related to user accounts [8]. Essentially, cybercriminals simultaneously try to deceive a larger number of victims in a fictitiously initiated data exchange that can reciprocally expose the personal data of the deceived persons, such as e.g. social security numbers [3].

5. CONCLUSION

Given that cybercriminals abuse information technologies in the online environment of the Internet's global communication network without space and time limitations, it is necessary to know how they commit such crimes in order to perform their effective and efficient detection and suppression.

Most fraudulent websites show a breach of privacy of any kind, including customer data, security of Internet users and financial information [7]. Because these websites rarely use any form of protection, customers and users of online services are often exposed to credit card fraud, identity theft and other forms of cyber fraud. [6].

Another risk is related to fraud related to consumer goods. Ads that claim to come from real companies that offer free products, such as toothbrushes and toothpaste or laundry detergent in exchange for filling out polls or some other type of public opinion poll by entering personal data into certain applications. The data collected by these means can then be used for further consumer fraud, such as identity theft and automatic telephone or electronic contact, performed by software created for the occasion.

REFERENCES

[1] Brussels, European Commission. (2020). Survey on Scams and Fraud – Final Report.

[2] Button, M. et al. (2014). Online frauds: Learning from victims why they fall for these scams. Australian & New Zealand Journal of Criminology, 47(3). pp. 391–408.

[3] Collins, S. M., Casey, R. P. (2020). Fighting Fraud. Washington D. C.: United States Senate.

[4] Hacket, R. (2017). Equifax Underestimated by 2.5 Million the Number of Potential Breach of Victims ., October 2. Preuzeto sa: http://fortune.com/2017/10/02/ equifax-credit-breach-total

[5] Koong, K. S. et al. (2012). An Examination of Internet Fraud Occurrences. The Univiersity of Texas – Pan American, January. pp. 441-449.

[6] Muncaster, P. (2017). Police:Buying Fake Goods Online Can Lead to ID Theft. Info Security, September26. Preuzeto sa: https://www.infosecurity-magazine.com/news/uk-policebuying-fake-goods-online/

[7] New York, Transnational Alliance to Combat Illicit Trade. (2020). Fraudulent Advertising Online: Emerging Risks and Consumer Fraud.

[8] Scam Alert: Con Artist Bank on Equifax Breach: (22.09.2017). Better Business Bureau for Marketplace Trust. Preuzeto sa: https://www.bbb.org/council/news-events/bbb-scam-alerts/2017/09/scamalert-con-artists-bank-on-equifax- breach

[9] Worobec, K. (2020). Fraud – The Facts 2020. London: UK Finance.