Multicultural Education

Volume 8, Issue 3, 2022

Cyber fraud (Internet- Related Fraud) crimes
Cyber Fraud in the Unregulated Foreign Exchange (FOREX) Scams Market as a Model
An Analytical &Rooting Study of the Saudi Legal System

Islam Mahrous Ali Naggi

Article Info

Article History

Received:
August 13, 2021

Accepted:
March 14, 2022

Keywords :
Crime, fraud, Cyber Fraud, Information Fraud, Fictitious Foreign Exchange Companies (FOREX), Foreign Exchange (FX)

DOI:
10.5281/zenodo.6353833

Abstract

This study aims to discuss one of the most important risk forms in money foreign currency exchange and investment that have spread in recent times. These are usually carried out by organized international gangs, unscrupulous dealers who deceive innocents, and steal their wealth by using cyber fraud. The study seeks to distinguish the criminal responsibility of the perpetrators of this form of criminal spear – phishing in the Kingdom of Saudi Arabia. The study also seeks to discuss prescribed penalties for these crimes in Saudi Arabia kingdom's jurisprudence.

The researcher followed the descriptive-analytical method to describe this phenomenon and analyze legal texts to determine its suitability and adequacy to study this sort of crime. The study discusses the concept of computer fraud, foreign exchange scam, foreign exchange entities, and the international organizations which grants licenses to these entities to practice foreign exchange activities and monitors them. Eventually, the researcher explains the penalties stipulated to be imposed on these entities under the Saudi Arabian kingdom jurisprudence.The study concludes with a set of ramifications and recommendations.

Introduction

The tremendous progress in information technology and the means of its transmission that accompanied the globalization of investments and markets have contributed to the diversity and multiplicity of forms of spear-phishing crimes. Spear-phishing crimes of foreign exchange **(FOREX)** fake entities are one of the most important of these crimes. Given that it is one of the most prominent dangers of investment, spear-phishing crimes of foreign exchange **(FOREX)** affects individuals' financial rights on one hand. On the other hand, the technological revolution has led to the globalization of crimes and the expansion of their implementation through the possibility of easily creating and promoting a website. Easily communicating with the investors and depositors, and the multiplicity of technological means to contact them, enable the perpetrators to entrap their victims. The statistics of cyber fraud crimes in The Saudi Arabia Kingdom during the last four years indicated that there are some close to thirteen thousand such crimes.

Therefore, the researcher's desire has grown to study the problem of fraud and cyber fraud crimes issued committed by unscrupulous operators and dealers of foreign exchange **(FOREX) scam entities.**

Methodology

The researcher used the descriptive and analytical method by describing the criminal phenomenon and analyzing the relevant legal texts to determine its suitability and adequacy for application to this type of crime.

Literature Review

1. The concept of Spear phishing

There are many jurisprudential definitions for the concept of spear-phishing crimes. Some define it as: "all fraudulent behaviors related to the use of computers, whereby the perpetrator's intention tends to achieve an illicit material profit**" (Al-Momani 2007).** While others went to define it as: "A fraudulent behavior related to spear phishing crimes process aims to achieve financial gain or interest" (**Al-Tawalbeh, 2008**). In survey research conducted in the United States of America, the survey defined the spear-phishing crimes as: "An act or a group of unlawful acts that are intentionally committed with the aim of deceiving or distorting to obtain something with valuable consideration, however using an electronic system law is mandatory to consider it as cyber fraud" (**Al Shawabkeh , 2004**).

Foreign exchange (FOREX) concepts

The Term **(FOREX)** is an abbreviation of the English term (Foreign Exchange), which means currency exchange **(Hebron, 2008)**. Foreign exchange **(FOREX)** is the largest financial market in the world, a large and decentralized market for currencies exchange, selling, and buying of most currencies. Most banks, institutions, individuals, and some companies are entitled to use foreign exchange **(FOREX)** markets **(Bin Ammar, 2008)**.

Foreign exchange (FOREX) scam entities

They are many entities not authorized to exercise any activity in **(FOREX)** markets, not qualified to act as a broker in the currency exchange activities and are not subject to the control of accredited international bodies to receive those victims' deposits. However, they do not credit these deposits in the real currency markets; they rather manipulate to create phishing websites via leased trading platforms **(Al-Jabra, 2002).**

These funds are credited to some unscrupulous peoples' accounts who will try to scam individuals through **(FOREX)** trading scams. These accounts are closed from time to time, re-opened in other names, and so on. Those **(FOREX)** gangs remit these funds through international overseas bank accounts to other countries, and they are exploited in various other illegal activities. Mostly, used with enterprises, gangs, mafias, and syndicates who are involved in organized crime of money laundering, or terroristic operations financing. Therefore, there is an urgent necessity for strict control procedures must be applied and followed by all countries over the word on these unregulated entities to put them under the watchful eyes of the relevant regulatory agencies to protect the world economy.

The procedures of licensing this type of financial entities in the Kingdom of Saudi Arabia are subject to the **Capital Market Authority** Law issued by Royal Decree No. (M / 30) on 2/6/1377 AH; and the regulations of the **Ministry of Commerce and Investment**, they are all strictly controlled systems. Despite all of that, many of these unregulated entities circumvent these procedures, establish branches in the Kingdom of Saudi Arabia purportedly with different forms of investment activities in the financial markets (such as training centers that provide training courses in economics and foreign exchange fields). Accordingly, they will not be subject to the control of the country watchdogs, and able to deceive people, having premises and commercial registry number in the name of the company without regard to the activity of this company listed in its registry.

This type of companies is also subject to many international regulatory agencies, including:

- **The Financial Services Authority (FSA):** It is established and subject to **The Financial Services Authority Act** of 2013 in **the United Kingdom**, which is concerned with regulating work in the financial markets; maintaining the efficiency of work in these markets; in addition to protecting investors from the manipulations and violations of these financial brokering companies. **The Financial Services Authority (FSA)** assists the investors to conclude fair deals, through the regulations that it issues. This body is also concerned with enforcing penalties on the companies violating its regulatory acts.
- **UK Financial Conduct Authority (FCA):**

It is an independent public entity, with statutory powers under the **Financial Services and Markets Act** 2000 which regulates the conduct of retail and wholesale financial services companies in the United Kingdom. The mission of this regulatory authority is to enhance the functioning of financial markets with the aim of protecting consumers, ameliorating market integrity, and encouraging competition(**Al-Tawalbeh, 2008**).

- **Cyprus Securities and Exchange Commission (CYSEC):**

Is the financial regulatory authority of the Republic of Cyprus, which was established in accordance with Article 5 of the (Establishment and Responsibilities) Act, issued by the Securities and Exchange Commission 2001. The aim of the Cyprus Securities and Exchange Commission (CYSEC) entity is to secure investor protection and facilitate sound development of the stock market through effective supervision**(Al-Ma'aytah, 2012)**.

- **Labuan Financial Services Authority (FSA):**

Labuan Financial Services Authority (FSA), a federal territory of Malaysia, is the central regulatory, supervisory, and executive authority for the international business and financial services sector. The Authority plays a vital role in ensuring that all International Business and Financial Centre IBFC entities in Malaysia are operating under the Labuan license are adhering to the highest financial standards**(Al Adinan; 2011)**.

Financial Sector Conduct Authority (FSCA):

Financial Sector Conduct Authority (FSCA) is the competent market authority in South Africa, which is responsible for enhancing the efficiency and soundness of financial markets. **Financial Sector Conduct Authority (FSCA)** promotes fair dealing for the clients by financial institutions and helps in maintaining financial stability.

Due to the presence of these entities of international and local oversight, these gangs manipulate to obtain permits for establishing companies with other activities than **foreign exchange (FOREX)** dealings. They exploit these companies in unregulated activities by establishing cyber fraud websites, by which they can attract innocent victims. They search carefully about the countries they can do phishing. They track and elect carefully the countries in which they will try to scam individuals **(FOREX)** trading scams. The citizens they seek about must enjoy a special wealth level, eager to obtain large profits, to be able to identify the appropriate fraudulent methods that can be used**(Al-Jabra, 2002)**.

1. **The Pillars of Electronic Fraud for (FOREX) Spear Phishing Dealers as a Model**.

The Saudi legislature did not specifically regulate the crime of cyber fraud through foreign exchange **(FOREX)** spear phishing companies. Rather, it was organized within the legislative framework for information crimes. The Saudi regulator emphasized in the fourth paragraph of the Information Fraud Management Act issued by the Royal Decree (M / 27) on 3/8/1428 AH, the criminalization of the cyber fraud and electronic fraud. The crime of establishing foreign exchange **(FOREX)** spear phishing entities for currency exchange is based on three main pillars.

The first one, which is the assumed the cornerstone, is the use of the internet or computers as the main tool of committing the crime via erecting a phishing website.

The second one: is the material element, which is committing cyber fraud, carried out by the perpetrator, and the result follows it and the **causal connection** between them. And at last:

The third one: is the moral element. The element is related mainly to the knowledge of the perpetrator, and his will to commit the crime.

We will discuss each corner separately to find out the availability of the elements of the crime against cyber fraud entities, or even legal entities that spoliation of citizens' wealth electronically.

The assumed cornerstone element: the execution of the crime through cyber fraud and phishing websites.

Internet fraud is the use of Internet services or software with Internet access to defraud victims or to otherwise take advantage of them is one of the most important, given that these crimes have a global character, and can be carried out in more than one country at the same time. The supposed element of this crime of internet fraud is the use of Internet services or software with Internet access to defraud victims or to otherwise take advantage of them. It is common to use tools as (computers, ATMs, credit cards, and mobile phones), let alone using malicious software, forged, or faked electronic documents. It is often carried out by organized and structured criminal groups consisting of three or more individuals, aiming to exploit the victim's need, to obtain a financial or material benefit from the perpetrator.

The Saudi regulator has put a specific definition of the information system Law in its first article of the act under combating information crimes and stated that: "It is a set of programs and tools designed to process, manage data and include computer sets". The legislator also specified a definition of the information network, stating that it is: "a link between more than one computer set or an information system Law to store and process data and exchange them with such private, public networks and with the World Wide Web.

And the legislator also defined computer programs, stating that they are: "A set of commands and functions that include directives or applications when running on the computer or computer networks perform the required outputs".

Accordingly, the **Foreign exchange fraud** gangs use computer programs and the World Wide Web to defraud individuals and spoil their wealth using phishing websites.

B - **The material element of the crime of cyber fraud in foreign exchange (FOREX) trading companies**.

The Saudi regulator has dealt with cyber fraud using computer devices by acting fraud crime prevention law under its procedural and substantive provisions. These provisions stipulated in the first paragraph of Article Four that: "Any individual commits any of the following information crimes, shall be punished with imprisonment for a period not exceeding three years and a fine of not less than Saudi riyals 2,000,000.- (only two million Saudi riyals), or one of these two penalties:

1- Seizing for himself or someone else the movable properties or bonds, or signing like that document, by fraud or impersonating a false name, or impersonating an incorrect character...

The material element of this crime is based on a group of elements, the first of which is criminal behavior that is a fraud, **assumption of name**, or impersonating an incorrect character. The last element is the existence of a **causal connection** between the perpetrator's behavior and the achieved result. We will discuss below the material elements to determine their suitability in the foreign exchange (FOREX) fraud crimes.

1. Fraudulent acts

The legislator did not set a specific definition of fraudulent methods, but the jurisprudence has settled on defining it as "any behavior that leads to the delusion, deception, and entrapment of a victim in the circle of fraud and intentional deception" **(El-Fil, 2011)**. A clear example is announcing a fictitious investment project.

Computer and internet fraud: It includes "the means used by the perpetrator to achieve the purpose of seizing the movable wealth or bonds or **sign bonds owned** by the victim" **(Al-Ma'aytah, 2012)**. And this method must involve fraud and deceit. Merely lying is not sufficient to prove fraudulent methods, regardless of the variety of their forms, so those lies must affect the conviction of the victim and make him give up his possession of money **(Nasr, 1994).** Accordingly, the crime of fraud is not achieved simply by false statements or allegations, but the perpetrator must support these lies with external manifestations that contribute to deceiving the victim and make him fancy the veracity of the lies presented to him by the perpetrator.

A clear example of such a case is if the perpetrator erected a website in a fake name bearing the company that he is marketing via it for foreign exchange **(FOREX)** transactions, and he was unable to communicate with the victims in this false cite bearing the name of the company. He uploaded several false photos and advertisements about his activity and the size of his business. Then, placed false assessments of fake clients who had made huge

profits, to instill confidence and entrap the victim. All these deceptive appearances were to facilitate the process of taking over the wealth of the victim after his deception. The evidence supporting the occurrence of the crime of electronic fraud is clear here.

It is also considered one of the fraudulent means that these phantom companies take to seize the victims' funds by persuading the victims to deposit sums of money, deposit them on fake platforms, and not the real one *MetaTrader* 4 (4 Mt). They rely on posting a fake simulation of the market through rented trading platforms and fool them with false hopes of making huge gains, promising them with even greater financial profits in the event of increasing their capital. The victim makes more deposits on this fake platform, and when requesting to withdraw the profits, these companies ask for insurance documents with amounts equivalent to the amounts of profits and original assets. Then, the company vanishes into thin air without they receive any money.

2 - Alias Name or Impersonation.

Alias Name: It is every name that the perpetrator assumes and is different from his real name - it is equal to the assumed name is a fictitious name in origin or a real name for a person other than the perpetrator and attributed to him to delude his victims that is his real name. It is not considered as alias name, the title he is famous for, and called by it. (**Abdelghani Samir; 2007**). Nor his real name included in the birth certificate, when it is other than his title famous name. Surly both names are considered valid **(Hafez; 2000)**. The **alias name** must be the one that makes the victim convinced to hand over his money, that is, there is a causal relationship. The causal relationship is between the bearing of the perpetrator the **alias name**, and convincing the victim to deposit his money at the perpetrator's end. If the name that was impersonated was not the reason that led the victim to deposit his funds, then the crime of fraud is not proven **(Harjah; 2004)**. Accordingly, it is an obvious example of this case of crime, whoever presents himself to the victim as one of the most distinguished economic figures in the world, and takes a specific famous figure name, and committed the crime of fraud by impersonating a false name of that distinguished economic figures to reassure the victim to hand him over his money. This is an important case in point**.**

The crime is based on the use of any fraudulent mean or assuming a false name or an incorrect description (**Zainuddin; 2008**). The material element of the swindling crime is achieved by any of them without the need to any more support it. Although it is most likely that there is the alias name or the impersonating of any other distinguished character or interference of any external factors, that may provide the means for fraudulent methods **(Al-Bahr; 2008)**.

Impersonate of other characters:

- Impersonation of other characters takes many forms and images. If the perpetrator falsely pretends to hold a scientific degree or being an expert in foreign exchanges **(FOREX)** in a global stock exchange market, or being a financial advisor, or claiming a special relationship, such as paternity, filiation, marital or kinship.

Like pretending to hold a position in the public service with intent to induce another to submit to such pretended official authority or otherwise to act in reliance upon that pretense to his prejudice (**Abdul-Ghani; 2007**).

Accordingly, an example of someone who claims to be a financial advisor to one of the important and influential global companies in the financial markets to deceive the victim and convince him that he is an expert in the world of financial markets and with his abilities to generates huge profits. This is clear evidence of fraud.

Legal relations are not considered a means of fraud because it is not an impersonation, even if it is false, such as someone who claims to be the owner of a plot of land or a company. An exception of that is the case of an agency, whoever falsely claims to be an agent of a global foreign exchange **(FOREX)** company that has a license and a good reputation in the financial markets if that leads the victim to hand him his wealth under the illusion of that false character. He has certainly committed the crime of fraud. The philosophy behind adopting alias name or the impersonating of any other distinguished character as a means to prove the crime of electronic fraud is based on that it indicates to the truthfulness of the lies that the perpetrator uses, to receive money from the victim, and the truth that the victim has no way to verify the alias name or the impersonating of any other distinguished character **(Al-Bahr; 2008)**.

Both methods are equal whether using alias name or the impersonating of any other distinguished character as a means of fraud, whether it is verbal or in writing the formal document. Besides, in the later, it may include a crime of forgery (**Harajah; 2004**). It is customary that if a person presented himself to another as being a lawyer or a doctor, he will not be asked for the university degree he obtained to check it **(Al Adinan; 2011)**.

It is required in both two aforementioned forms, that the alias name or the impersonating of any other distinguished character must be accompanied by a positive action from the part of the perpetrator to be judged as a crime. If the victim hands the money to the perpetrator by mistake believing that he is another person, then the accusation crime does not take place here, because the recipient is not supposed to notify the victim of such mistake **(Zinedine; 2008)**. For example, if the victim hands over his money to a person whom he mistakenly believes he is an agent for one of the international money exchange companies, and without engaging in any positive behavior from the latter, then a fraud crime is not committed in this case.

3- **Corpus delicti**

The Saudi legislator explicitly stated the **corpus delicti** of this crime and the object of its protection. The legislator decided that it is the movable assets and bonds, and signing the power of alienation form must be the final goal of the perpetrator to collect the remitted funds. Hence, it is not suitable for the **corpus delicti** to be a real estate such as an apartment, or land for example. Rather, it is suitable for **corpus delicti** to be on the apartment contract as a movable bond asset with a financial value. An example of this is when a representative of this like this fraud entity persuades the victim to hand him over a sum of money for trading in the foreign exchange **(FOREX)** market, and the latter delivers money or a contract of an apartment, check, or debt bond, as a result of the fraudulent methods used by the perpetrator, then there is a **corpus delicti** of the fraud crime against the perpetrator. The amount of this money does not matter, if funds are much or less amount, it will not affect the crime (**Zain Al-Din; 2008**). However, the amount of money is one of the considerations that the trial court relies on to issue its judgment, and called reasons for judgment.

The intent of the perpetrator must be directed towards seizing the victim's money which is not owned to him. The lessons learned here are that the truth and reality are what is important here. If the money is the property of the one who seizes it, then there is no crime in his act, even if he thinks at that time that he is seizing money owned by the others **(Sorour; 2003).**

4- **The ruling on attempting to commit the crime**

Article 10 of the legal system states that: "Whoever attempts to commit any of the crimes stipulated in this legal system shall be punished not exceeding half of the higher limit of the prescribed penalty.

The legal system has adopted in this text the rule established in the Islamic Sharia, which is adopted by some Man-Made laws. This rule states that there must be an unequal punishment between premeditated complete crime and an **inchoate offense** or attempted crime, which should have a lower penalty. This is on the basis that attempting a crime does not infringe upon the right protected by the law, but it is limited to merely threatening it. This means that and an inchoate offense is less harmful to society than outright crime, consequently, there is a need for inequality between the complete crime and the mere attempt to commit the crime (**Sorour, 2003**). As an example, if the perpetrator created a website for **a foreign exchange (FOREX)** company and used it to collect the data of his victims, but while trying to convince his victim to deposit his wealth at his end, the victim discovered his lack of credibility, refused to deposit his money or informed the concerned authorities. Here, in this case, it is considered that the crime ceased to take place; it was only an **inchoate offense** or an attempted crime.

The preparatory actions must be distinguished when committing the crime. The description of the previous case for the crime of electronic fraud is considered a preparatory act for every activity that the perpetrator undertook before using fraudulent means. As a vivid example of this case, preparatory actions are to prepare software programs via which individuals will register on the site, preparing fake images that as an advertisement for the fictitious entity, and preparing false customer comments praising in the fictitious entity **(Nasr, 1994).**

The preparatory work ends at the moment when the perpetrator connects the computer or his mobile phone to upload these programs, pictures, and false comments on the site. The start of operating programs and uploading pictures and comments are considered an attempt to commit the crime.

5- Criminal outcome

The criminal consequences are the changes that take place in the outside world as a result of the offender's behavior **(Al-Jabra; 2012)**. The result of using fraudulent methods as described by the judicial system Law is the appropriation of movable assets or bonds, or the **assignment** of these bonds favor of the perpetrator, by deluding the victim of wealth and entrapping him. The result is that the victim handles all or some of his wealth to the perpetrator. The crime will not be completed unless the result is achieved, and accordingly, leaving the transferred money or bond from the victim's possession to the perpetrator's possession, then the crime is completed and he must be punished according to the law.

6- The causal relationship between the means of fraud and remitting the victim's money

For the existence of the causal relationship in the cyber fraud crimes in foreign exchange **(FOREX)** scams, the remittance of money or assignment of the bonds is a result of the perpetrator's behavior and the deceptive fraudulent methods used to delude the victim with the dream of getting rich quickly. If the result is not due to this fraudulent behavior, the causation link is null.

Also, the fraudulent method must be before handing over the money, and if that was not the case, and the fraudulent method used by the perpetrator did not affect the victim, nor was it the reason for his handing over the money to the perpetrator, and the victim would have delivered the money to him whether the perpetrator used the fraudulent means or not. Then, the fraudulent method was not used and there is no crime of swindling in this case (**Abdel-Ghani; 2007**). As an example, if the perpetrator persuades the victim to hand over his money to invest it in the foreign exchange market, and as a result of the victim who has been tricked by the company's representative, that the company will provide a special program for new clients by granting them additional credit balance (as a bonus) equivalent to the same balance of his deposits. Accordingly, the victim's

deliver them his money as a result of this fraudulent method. It is clear that this case includes material elements of cyber fraud crimes against the perpetrator.

C. The moral element of the crime of cyber fraud

The crime of cyber fraud is intentional, and to prove, the presence of criminal intent against the perpetrator is required. Moreover, it is not sufficient to have general criminal intent only, but it must be established alongside the presence of private criminal intent. Then, if the private intent is absent, the crime ceases to be found.

1. General criminal intent

The general intent in the crime of cyber fraud can be proved by the main two elements, the element of knowledge and the element of the will. To prove the occurrence of the crime, both elements must exist together: the perpetrator must be well aware that he is committing a crime when he posts data and information into the computer or the mobile phone software systems for huge false gains and profits to extract funds from the victims. He is certainly committing the crime of electronic cyber fraud **(Nasr, 1994).** Besides, his free and chosen will must be directed to fraud the victim without any shadow of a doubt (**Al-Ma`aytah; 2012**). As an application to this case, if the perpetrator requests the confidential password numbers of the victim's credit card, withdraws his balance, after the victim was handed him over secret password numbers after he was fooled with misleading earnings data provided by the perpetrator. Then the criminal intent of the cyber fraud crime has been established against the perpetrator.

2. Private intent

It is also a condition to prove that there is a crime that must be a special criminal intent, which is the intention of the perpetrator to seize the full possession of the transmitted funds or the assignment of the bonds by the victim's favor of the perpetrator. If the perpetrator's intent is not to possess or seize the victim's money, then there is no criminal intent. Proving the private criminal intent of the fraudulent perpetrator is a matter based on the facts of the case and the conclusions drawn from it by the trial court **(Al-Hadithi, 1996).**

D. **Punishment for the crime of cyber electronic fraud for fictitious Foreign Exchange (FOREX) companies.**

1. **The original punishment**

The crime of electronic fraud for **foreign exchange (FOREX) companies** is considered one of the major crimes requiring the arrest of the perpetrator, and stipulated in Resolution number (2000), of The Saudi Interior Minister dated on 06/10/1435 AH. The legislator assigned a sentence of 24 hours up to three years in jail and a fine of not more than two million Saudi riyals for the crime perpetrator. The legislator also granted the trial judge the authority to distinguish between the imposition of imprisonment or a fine, or both, according to the facts of the case, the fraudulent means used by the perpetrator, and the harm that inflicted on the victim.

2. **Supplementary punishment**

Article thirteen of the Cybercrime Law stipulated the complementary punishment stated that it the confiscation of the devices, programs, all means used in committing the crime, and the funds collected due to committing this crime. Besides, it granted the competent court the authority to close the website or the place of service provision that was the source of the crime to be closed permanently or temporarily.

3. **Inflicting The Tougher penalty**

Article 8 of the Cyber Crime Law specified cases of **inflicting more tough penalties**, stated that: "The prison sentence or the fine shall not be less than half of its higher limit if the crime is associated with any of the following cases acts ....").

The Law stated specific cases, in which the judge is restricted to apply the tougher penalty, due to the availability of the aggravating circumstances so that the minimum penalty prescribed must not be strictly the minimum penalty, but rather half of the maximum limit for the original penalty included (imprisonment and fine) or one of those two penalties. These cases were mentioned by the legislator exclusively and not as an example, namely:

- If the perpetrator committed the crime in cahoots with an organized gang.
- That the perpetrator occupies a public office, and the crime has a relation to his position, or he committed the crime by exploiting his powers or influence.
- Deceiving and exploiting minors and those who are like them.
- **The issuance of previous** sentences, at home, or abroad against the perpetrator of similar crimes, or what is described in the public penal law as the case of "habitual criminal".

Accordingly, the crimes of electronic cyber fraud that are committed by organized gangs should be punished by more tough sentences applied to the perpetrator, the prison or fine sentence will not be less than half of its maximum sentence.

Conclusion

1. The Saudi legislator has not specifically addressed the cases of foreign exchange **(FOREX)** scams' entities.
2. The crime of electronic fraud for fictitious foreign exchange **(FOREX)** scams' entities is one of the most sophisticated crimes. It is in line with scientific and technical progress, and it depends on the intelligence of the fraudster and the desire of the victim to get rich quickly.
3. The crime of electronic fraud for fictitious foreign exchange **(FOREX)** scam is the cornerstone of two crimes associated with it, the electronic crime itself is a tool for committing the crime directly or indirectly, and the crime of money laundering obtained from it to conceal its true source and origin.
4. The absence of strict control measures for publishing fake ads for foreign exchange **(FOREX)** entities, contributed to increasing their numbers.
5. The current criminalization of the crime of electronic cyber fraud act, for fictitious foreign exchange **(FOREX)** entities, is not appropriate in terms of both conditioning the crime or the insufficiency of the prescribed penalty to help confront this type of sophisticated crime.
6. The necessity to impose strict control measures on the foreign exchange **(FOREX)** services providers, especially concerning publishing electronic promoting ads, with empty promises of gaining a quick huge fortune.
7. Prompting of issuing a new legal legislation system that deals with foreign exchange **(FOREX)** and investment crimes, at the same time, new strict severe penalties must be appliedfor this type of organized international sophisticated crimes.
8. Concluding new international agreements between the Kingdom of Saudi Arabia and the countries in which like these types of crimes implementation is easy to spread. Moreover, to coordinate to apply a law that could help in limiting such crimes. Extradition agreements must be concluded with such countries, the agreements must include binding clauses to return the seized funds.
9. Activating the role of the media outlets, to contribute to spreading awareness to reach the largest possible number of citizens in the Kingdom of Saudi Arabia territories.

References

Bin Ammar; Mughni (2018), *The Concept of Economic Crime in Comparative Law*, Al Basera Center for Research, Consultation and Educational Services, Issue No. 11.

Al Ma'atah; Hamza Atef Ali (2012), *The Crime of Electronic Fraud, a comparative analytical study* - Master Thesis - Mutah University, Jordan.

Algebra; Ali Awad (2012), *The Crime of Fraud in the Field of foreign exchange ((**FOREX**)) in Local and Foreign Stock Exchanges*, A Comparative Study, Ph.D. Thesis, Ain Shams University, Egypt.

Al Feel; Ali Adnan (2012), *Cyber - crime*, first edition, Zain Human Rights Publications, Beirut, Lebanon.

Al Odainan Abdullah Muhammad (2011), *Information Fraud*, The Excellence Center for Information Security, available on their website: www.coela.edu.sa

Al Khlil; Ahmed Bin Muhammad (2008), *Stock Exchange Systemic Crimes and their Jurisprudence Provisions*, The Journal of Sharia Sciences, Imam Muhammad Bin Saud Islamic University, Kingdom of Saudi Arabia.

Zain Eldine; Bilal (2008), *Crimes of Automated Data Processing Systems*, First Edition, Alfikr Al Gamiee Publishing House, Alexandria, Egypt.

Al Bahr; Mamdouh Khalil (2008), *Crimes About Money in the UAE Penal Code*, First Edition, Thara' a Publishing House, Amman, Jordan.

Al Towallyia; Ali Hassan (2008), *Cyber - crimes*, First Edition, Applied Science University, Bahrain.

Momani; Nahla Abdel Qader (2007), *Information Crimes*, First EditionDar Al Thakafaawa Al Nashr, Amman, Jordan.

Abdul Ghani; Samir (2007), *Financial crimes*, Shatat Publishing House, Cairo, Egypt.

Shawabkeh; Muhammad Amin (2004), *Computer and Internet Crimes (Information Crime)*, First Edition, Dar Al Thakafaa for Publishing, Amman, Jordan.

Hargah; Mostafa Magdy (2004), *Crimes of fraud, breach of trust and associated crimes*, Mahmoud Publishing House, Alexandria, Egypt.

Hafiz; Magdy Moheb (2000), *Crimes of Deception, Fraud, and Other Crimes linked to them*, Legal Books House for Publishing, Alexandria, Egypt.

Al Hadithi; Fakhry (1996), *Explanation of the Penal Code* - Special Section - First Edition, Baghdad, Al - Zaman Press.

Nasr; Samiha (1994), *Trends Toward The Crisis of investing money Companies and Its Relation to In - Kind Values of Affected and Unaffected People*, Seminar on New Economic Crimes, National Center for Social and Criminal Research, Crime Research Department, Cairo, 20-21 April 1993 - Part One.

Author Information

Dr. Islam Mahrous Ali Naggi
Assistant Professor of public Criminal Law,
Department of Public law
Collage of Law
Princess Nourahbint Abdulrahman University
Riyadh, Saudi Arabia