Financial Identity Theft In Alegria legislation
سرقة الهوية المالية في التشريع الجزائري

Boukhalfa hadda ♦
Oum El Bouaghi University / Algeria
hadda.boukhalfa@univ-oeb.dz

Date of submission: 25/11/2023 Date of acceptance: 28/03/2024
Date of publication: 30/06/2024

Abstract:

financial identity is a copy of personal data attached to the client, which expresses its financial position in its dealings with financial institutions and business companies which increased its value with increased economic trading and recent developments in the field of information technology, it needs legal protection from various attacks. Due to these attacks, which affect clients' financial privacy, extortion, defamation and exploitation of their funds, and thus expose them to legal problems

This paper aims to determine the nature of the offence of theft of financial identity in Algerian legislation and to address the most important forms of attacks on financial statements by theft.

Keywords: financial identity, financial position, theft offence, dealer, financial privacy.

الملخص :

تعتبر الهوية المالية صورة من البيانات الشخصية اللصيقة بالمتعامل، و التي تعبر عن مركزه المالي في تعاملاته مع المؤسسات المالية و الشركات التجارية، و التي زادت قيمتها مع زيادة التداولات الاقتصادية و التطورات الحديثة في مجال تكنولوجيا المعلومات، و التي تحتاج لإضفاء حماية قانونية لها من مختلف الاعتداءات الواقعة عليها. و نظرا لهذه الاعتداءات التي مست الخصوصية المالية للمتعاملين و ابتزازهم و التشهير بهم و استغلال أموالهم و كذا تعريضهم للمشاكل القانونية.

و تهدف هذه الورقة البحثية لتحديد معالم طبيعة جريمة سرقة الهوية المالية في التشريع الجزائري، و التطرق لأهم صور الاعتداءات الواقعة على البيانات المالية بالسرقة.

♦ **Author Sent**

الكلمات المفتاحية : الهوية المالية ، المركز المالي، جريمة السرقة ، المتعامل ، الخصوصية المالية.

Introduction:

Financial identity data of clients with financial institutions and commercial companies is of great importance in completing their transactions the customer uses this data to access their personal accounts, control all related transactions and make requests for banking transactions, for financial institutions such as banks or commercial companies, they rely on financial identity data to basically identify customers' personality. Verify their validity and then respond to them with regard to confirmation of transactions, orders and the provision of financial services to customers.

Abuse of the right to private life appears in many spheres of life the financial identity of a person is one of the most important personal data that is subjected to attacks, especially with the recent technological development, there are a range of offences against financial information, which begin with the theft of financial identity data and its use for financial gain or any other criminal activity. Also, the theft of such data does not affect the security and right to privacy of the financial identity of the client only but they affect the security of the financial institutions and the business companies that deal with them as well.

The importance of this position lies in the general interest in information by technology makers and has been developed from many technologies to trade this information, develop its use and benefit from it securely, quickly and most importantly confidentially.

The legislator interest in providing the necessary legal protection for the circulation of such data from the author, holder or persons using it in its dealings with the dealer, in order to achieve the legal security of financial information from the various attacks that occur.

This study aims to determine the nature of the theft of financial identity data, identify the concept of financial identity as the subject of this crime, and then address the forms of the theft of financial identity data.

The problems of studying: **what are the features of the theft of financial identity data in Algerian legislation?**

It is what we will try to highlight according to an analytical legal study, through which we can view Forms of theft of financial identity.

In the light of the above, we have decided to divide the subject matter of this study, in accordance with the following plan:

First: Normalization of the Crime of Theft of Financial Identity

Second : Forms of theft of financial identity

Chapter I: The Nature of the Crime of Theft of Financial Identity

We must begin by clarifying what this crime is, in terms of defining it and identifying the method used by the aggressor to carry it out.

1- disclosure of financial identity theft

The definition of financial identity theft, and the methods used by the aggressor in obtaining data, will be addressed.

Section I: Definition of identity theft

Some jurists defined the theft of customer data as misuse of another person's financial identity data, such as account numbers, date of birth and email address, without his knowledge or consent. It is also defined as the use of a person's data, such as name, social security number and credit card number, without his or her consent to fraud or other offences[1].

It has also been defined as an Internet-linked computer hack with the intention of stealing the data and data stored therein, such as penetrating the networks of financial banks and banks to make illegal bank transfers[2].

It should be noted, however, that previous definitions have linked the act of using such data to poor use. financial identification data ", where the trespasser, after obtaining the financial identity data, treats it as the owner, These tariffs combine the act of obtaining financial identity data with the act of unlawful use. and stresses the need to meet these two acts to achieve theft, which results in harm to the client, whether physical or moral.

However, a theft of a financial identity may occur simply by consulting it as well, as it expresses the true Form of the client not only in material terms but also in personal terms, which causes harm to the aggressor's conviction to enter and access financial information even if it is not used, thus punishing the attempted theft. Because this is an infringement of the right to privacy protected by the law, and it must not go beyond theft for the act of seizure or even the act of use. The damage is done here as soon as such data is disclosed without the permission of the owner and without the authorization of the authorities concerned legally.

[1] Suleiman bin Abdul Razek, Forms of Cyber Extortion Crimes and Their Motives and Psychological Implications, Security Research Journal, King Fahd Security College, vol. 27, No. 29, 2018,p173.

[2] Alaa al-Tamimi, Legal Organization of the Online Bank, New University House, Alexandria, 2012,p604.

Financial Identity Theft In Alegria legislation

Unlawful access to financial data and information containing customers' secrets is kept confidentially, the owner of which wants confidentiality and is not permitted, and any hack and disclosure of such data using illicit means may expose the trespasser to legal accountability for the crime of attempted theft.

It can be said that financial identity theft is the seizure and unlawful exploitation by a person of a transaction's financial statements that he uses to dispose of his money and perform his financial transactions.

It can also be defined as: a person accessing the client's financial statements, using them in his own interest and realizing the gains, by pretending to be the real financial data holder, after hacking, disclosing and using them to damage the client with financial identity.

The crime here is not only focused on seizing financial identity information, but can also be associated with the illicit exploitation and use of it to damage the owner's financial identity.

The term theft does not mean the transfer of such data away from the dealer, but goes beyond other concepts that include every assault on such data with the intention of illicitly exploiting it.

Section II: Methods of theft of financial identity data

The theft of the client's financial identity data takes place in one of the following ways[1]:

- The aggressor sent fake emails to the dealer, depicting them as coming from the bank or business company, where in these messages they request to send the client's password, or account numbers, for example by wanting to delete such data from the financial institution's database because of a fault.
- The aggressor installs devices that monitor the customer's behaviors and dealings with all the tools he can use to communicate with the bank or trading company, such as his personal computer, or cash withdrawal machines. The aggressor is able to obtain such data in one of two ways: either to capture such data while it is being sent unsafe, or to install a software on the device of the person who wants to steal his personal data, so that the program collects such data and automatically transmits it to the person who has installed it.
- The aggressor's use of fraudulent means, such as the establishment of a website, And to offer fake products or services through this site And they ask the bank dealer to enter details of his name, And his email address, and

[1] Alaa al-Tamimi, op. cit., p. 606.

his bank account numbers to get the advertised commodity or service, He then exploits this data in dealing with the bank or business company.

- The aggressor searches the papers, documents or invoices of the dealer, for details of his personal data, which can be used in dealing with the bank or business company.

2- Financial identity theft

We must define the concept and type of data that is being assaulted and its most important characteristics.

Section I: Definition of financial identity

The importance of identifying what a financial identity is because it is the subject of the crime of theft of a financial identity, which results in a lot of security infringements that are detrimental to the owner of this information and the persons dealing with it and even banks and commercial companies, for this purpose we stand to define the concept of this financial identity.

Financial identity is defined as the specific data of the person, such as the amount of the balance of the open credits, the maturity dates of his debts and his budget numbers, the request to defer the fulfilment of his debts, and whether or not he has an account with the bank[1].

The data of the Bank's customers are characterized by the fact that they do not relate to the personality of the owner, which is the opposite of the biometric characteristics such as fingerprint, and voice frequency, which allows the use of such data by the owner, or others who know about it[2].

Financial identity includes all relevant information to the client, representing his or her income, disbursements, disbursements of such funds, his or her place of business, home address, postal address, email address, telephone numbers, career status, financial status, credit record, and other personal information accompanying the client's financial identity.

The financial identity of the customer is also the financial reputation of banks, insurance companies, facilities and commercial reputation of the local and global market and of the Chamber of Commerce and Industry, that

[1] Ali Jamaluddin Awad, Banking Operations from Legal Point of View, Edition3, Arab Renaissance Publishing and Distribution House, Cairo, 2000,p1084.

[2] Alaa al-Tamimi, op. cit., p. 598.

is, everything that falls within the scope of financial disclosure is based on the financial personal balance and its obligations[1].

The financial data are: customer records, credit card information, data operating methodologies, such as usernames and passwords, human resources records, employee data and private documents stored on the computers of financial institutions and commercial companies.

Summary of the above financial identity can be defined as such data and information relating to the financial life of the customer, which determines the scope of his dealings with financial institutions and business companies.

Section II: Characteristics of financial identity

Financial identity has a range of characteristics, namely:

a- Financial identity attached to the client:

The right to financial identity data and information is not exercised by the owner. rights ", who considers this right to be one of the inherent rights of the recipient, However, the agent of the holder of the right to privacy is fully competent to exercise proceedings in relation to the infringement of the latter's right to the inviolability of his financial information provided that the agency is explicit In the sense that a human being's personal entity is embodied in two elements, one natural and the other legal, The natural element is embodied in the human person in terms of membership, psychology and mentality. and the legal element of rights inherent in personality determined by law, Such as the right to name, Form, and the right to honour and consideration and the right to privacy, including the inviolability of assaulting financial identity data[2].

b- Financial identity is not waivable:

The right to financial identity may not be waived or disposed of waiver, whether temporary or absolute, or express or implied financial identification data cannot be a place of sale, gift or will, He does not envisage a change in the right holder's financial identity. or dispose of the legal protection established for it by the disposition of that right[3].

The information is classified as personal data even if it becomes publicly available by waiver from the person with the statement ", for example when

[1] Zainab Star Jabbar Kazem Al-Lami, Civil Protection of Personal Data Online, Comparative Study, Misan Journal of Comparative Legal Studies, vol. 1, No. 5, Iraq,p140.

[2] Rafie Khader Saleh, Zina Sahib Curran, Restriction of Right to Information, Comparative Study, Al-Halabi Investigator Journal of Legal and Political Sciences, Issue 2, year 10, Baghdad, 2018,p. 198.

[3] Zainab Star Jabbar Kazim Allami, op. cit., p. 144.

filling out forms for a service or job here a person cedes a set of financial identity statements for receiving the service, Here the service provider has the right to exploit this data by searching or registering But this is only conditional on the limits of the service provided and this is not an infringement of financial identity data, On the other hand, this waiver does not amount to the removal of the disclosed financial identity data. Data is considered personal data, even if not accurate or incorrect[1].

c- Digitization of financial identity:

Transmitted and exchanged data, which are termed many expressions in the Internet environment as the flowing river of information Internet protocol address for individual computers, browsers used, type of computer used, And the last thing the user did on his recent visit to the site and possibly other sites he visited information, which may be sufficient to identify a person, is caught and collected at many points in the journey through networks.

They may be available for reuse, disclosure or transfer between sectors concerned with their collection and some of this information may be important and necessary for web operations and access to websites, Like a telephone number and a private IP address, without which the network is unable to operate, But there are pieces of information that may not be necessary for these operations and may be collected for purposes other than network operations and with information collected at the stages of purchasing products or simply to register or subscribe to the services of the site, The collection of such information may constitute an account of an individual's activities, and at some stage such data, when collected and analysed, becomes material that reveals many details that a person may not wish to disclose. At the same time, these data become rich material and a place of sale for business and activities purposes[2].

Chapter II: Forms of theft of financial identity

The offence of theft of financial identity includes various Forms of attacks against its data.

1- Financial Identity Grabbing Offences

The offence of theft of financial identity is especially apparent in a series of criminal acts committed by the aggressor .

[1] Marwa Zayn al-Abidin Saleh, International Legal Protection of Personal Data Online between International Convention Law and National Law, Center for Arab Studies, Egypt, 2016, p. 73.

[2] Mona Turki Al-Mousawi, Information Privacy and its Importance and Risks of Modern Technologies, Baghdad College of Economic Sciences Journal, Special Issue, Baghdad, 2013, p. 53.

Financial Identity Theft In Alegria legislation

Section I: Illicit collection of financial identity data

The collection of the financial identity data of the client is illegal in two cases: first, the use of fraud, fraud and eavesdropping in order to obtain that information, in addition to not knowing the author of that collection, and second, the collection of data prohibited by law, which establishes technical or legal controls governing the collection or storage of such financial information as the client[1].

Under article 59 of Act No. 18-07[2], the offence of gathering data using illegal methods is punishable by 1 to 3 years' imprisonment and a fine of 100,000 to 300,000 DZD for collecting personal data in a fraudulent, dishonest or unlawful manner. This offence is the use of illegal methods by the aggressor responsible for processing when collecting personal data.

In Algerian legislation, in the absence of a provision to protect financial identity data against aggressors, indirect protection of financial privacy can be provided through articles 394 bis to 394 bis 7 ofcriminal code No. 04-15[3], under a new chapter entitled: Infringement of automated data processing systems in which the legislator criminalized activities or acts that are an assault on automated data processing systems, with the aim of protecting automated processing systems .

It seems obvious that data or data relating to financial identity are not referred to from near or far because the text is intended to protect processing systems per se, but criminal acts involving processing systems infect the data and data processed, which may be the financial identity of which the criminal description applies, thereby granting them protection like other data.

In addition to Law No. 15-04[4] on Electronic Signature and Certification, in which the legislator set out the general rules on electronic signature and certification, That requires the collection of certain financial identity data, article 05 of which stipulates that the databases collected must be located within the national territory.

The collection process is carried out in a number of ways, including:

---

[1] Zainab Star Jabbar Kazim Allami, op. cit., p. 144.

[2] Act No. 18-07 of 10 June 2018 on the protection of natural persons in the handling of personal data, Official Journal No. 34 of 10 June 2018.

[3] Act No. 04-15 of 10 November 2004, containing thecriminal Code, Official Journal No. 71 of 10 November 2004.

[4] Act No. 15-04 of 01 February 2015, containing the General Rules on Electronic Signature and Certification, JR No. 06 of 10 February 2015.

a- Search offence:

"Unlawful search" means information and data that are used illegally to abuse the financial identity and data within it. the perpetrator of this crime is aware of the illegality of what he is doing and nevertheless his will tends to offend the financial identity of the client, It may be meant to search for information hacking using malware to hack and collect information from a system that contains financial identity.

b- Capture offence

Capture is intended to obtain information exchanged between persons Whether written, audio or video, modern and online technologies can exchange their conversations either by writing like email or by audio and photo like Instagram. s knowledge or consent is a punishable offence, whether by traditional or modern methods.

Unlawful data capture is unlawful access to a particular information system, such as a system for banks or vendors, so that the offender can capture customers' financial identity data through the channels of communication thereafter, through information espionage or fraud[1].

c- Registration or transfer:

Registration means the copying and preservation of financial identity data between the client and the financial institutions or business companies in any way on a device or any other means prepared for this. For transportation, it is intended to transmit this data that has been recorded from the device or channel that has been used to another channel, CNC and via the Internet or any other conventional device.

The Algerian legislature has linked these acts to the interdependence of the criminal act between them and the result thereof. And it stipulates that this assault falls on the secret and private conversations of victims that are part of their private lives that they wish to be closed and undeclared to others, It may also include all confidential and archived data of the client affecting the client's financial identity.

Section II: Hacking of financial identity data

The crime of hacking is one of the most important forms of assaulting the financial identity, as it affects the systems and devices containing the financial identity data of the client, as follows.

[1] Mohammed Amin Ahmed Al Shawabneh, Computer and Internet Crime, Edition1, Culture Publishing House, Jordan, 2004, p. 166.

Financial Identity Theft In Alegria legislation

a- Offence of unlawful entry

Unlawful entry means the process of access to information systems without the permission of the owner, and is also defined as access to the information system without the authorization of the computer or information owner[1], or "It is the misuse of the computer and its system by an unauthorized person to access the information and data stored inside it, to access it or simply to entertain it, or to satisfy the feeling of success in hacking the computer."[2] "Unauthorized access to the computer system derives from its illegality being unauthorized or contrary to the provisions of the law."[3]

Article 394 bis of the Algeriancriminal Code[4] stipulates the offence of entering into information regulations, as amended, and the legislator uses the term "fraud" in this offence to indicate that such entry is unlawful, as provided for in this article. "... whoever enters or stays through fraud in all or part of the automated data processing system or attempts to do so."

"The term fraud means that it is done in a fraudulent manner by not possessing the right to access, password or any legal electronic procedure used by the owners of this system. Thus, any person who enters an information system in part or all of it is considered unlawful and the crime of entry is punishable.Some legal legislation and jurists therefore use the term hack to indicate the illegality of access to the information system."[5]

It should be noted that until the crime of illegal entry is completed, must have the criminal intent and the element of science and will, The actor must be aware of the illegality of his entry act. The aggressor who is a bank employee or a commercial worker knows the places and time to which he is authorized to enter and the powers conferred upon him. and, if he enters another place or for a longer period of time, this proves the criminal intent of his right to unlawful entry into the system.

b- Fraudulent Survival

Fraudulent survival is the process that follows the process of accessing the system, whether it is legitimate or unlawful, and therefore it is anyone

---

[1] David Bainbridge, Hacking (The Unauthorised Access of Computer Systems) - the Legal Implications -, The Modern Law Review, Volume 52, Issue 2,March 1989,p 237.

[2] Naila Adel Mohamed Farid Qura, Economic Computer Crimes - Theoretical and Applied Study -, Edition 1, Halabi Rights Publications, Lebanon, 2005, p. 326.

[3] Ibid., p. 319.

[4] Act No. 04-15, amending thecriminal Code.

[5] Fashar Attallah, Confronting Information Crime in Algerian Legislation, Maghreb Forum on Law and Informatics, October 2009, Academy of Postgraduate Studies, Libya, p. 23.

entering and staying fraudulently in the information systems and in bad faith. It is defined as "being within the automated processing system against the will of those who have the right to control it"[1]. It can also be defined as any unlawful presence in an information system, whether with the intention to sabotage it or not, enough to have a person present for a period of time.

Survival is that the perpetrator does not disconnect with the system when he realizes that his presence is illegal. It starts from that moment when the person should have changed his status by leaving the system. "The offence of unlawful stay within the information system is generally considered to be an offence that is difficult to substantiate, with the accused alleging in the event of arrest that he was about to break away from the infringed regime."[2]

However, for a bank employee or a business worker who is authorized to enter the information system, the process of staying here must exceed the duration of their duties And the meaning of this is that these people are authorized to enter and stay in the systems, but this is for a certain purpose, When he finishes his technical operations, he has to leave and terminate the entry process. The aggressor here has overstepped the permit by continuing to remain in the system beyond his prescribed time.

Article 394 bis of the Algeriancriminal Code[3] explicitly stipulates that the offence of unlawful presence in information systems must be a deliberate offence, as follows: "Anyone who enters or remains through fraud...".

2- offences of exploitation of financial identity

Stolen assault is not only about taking financial statements, but also about exploiting them and using them by the aggressor for financial gain.

Section I. Illicit use of financial identity data

The unlawful use of financial identity data appears in a variety of criminal behaviours as follows:

First, crimes of destruction:

stipulated by Algerian legislation in article 394 bis 1 of thecriminal Code[4].

[1] Ali Abdelkader Qahouji,criminal Protection of Electronic Data, Law, Computer and Internet Conference, May 1-3, 2000, Faculty of Sharia and Law, United Arab Emirates University, Abu Dhabi, p. 52.

[2] Nhla Abdelkader Al-Momani, Information Crime, Edition 2, Culture Publishing and Distribution House, Jordan, 2010,p. 161.

[3] Law No. 04-15.

[4] Ordinance No. 66-156, containing thecriminal Code.

a- Entry: The entry means the addition of new data on the client's financial identity, whether it is empty or previously available. And this act is achieved for the purpose in which the legitimate holder of the magnetic debit cards is used, The latter withdraws cash from ATMs when it uses its own and secret number to enter to withdraw more money than the amount in its account[1].

The entry here changes the data and information in the system used and can also change the way the software in which the system operates, resulting in a change in the entire system. The aggressor may enter fictitious data or information enabling him to seize financial identity data that often relates to financial elements in order to make money for himself.

b- Erasure (removal): Erasure means removing part of the data inside the financial identity, or transferring it and storing it elsewhere. This process here alters the content of the financial identity[2].

The Algerian legislature has not specified the manner in which the act of removal is carried out, whether it is done with a special program or only by means of a key or an erasure icon, nor has it indicated what kind of data or information is erased, and sometimes erasure may be by distinguishing certain data or information contained in or operated by the financial identity system.

c- Modification: The modification means the change of the financial identity data, which either replaces it or adds other data other than it; Or the modification is also by changing the program in which the financial identity data is processed by another similar or different program The aggressor breaches the ports and accesses the database, And modify it or add the false information in order to illegally benefit from that data.

The aggressor's criminal intention is to change his financial identity by adding, deleting, or transferring data, software, viruses or operating systems from one system to another. The physical element is as soon as there is a change in the financial identity data, the criminal conduct is to assault the financial identity data by adversely affecting it and in any way modifying its content[3].

[1] Fachar Attallah, op. cit., p. 30.
[2] Ibid., p. 30.
[3] Ibid., p. 31.

Second, crimes of disposal of financial identity data:

The theft of financial identity data goes beyond disposal and exploitation, as follows:

a - Customer Account Control

The aggressor after seizing all financial identity data of the customer's account by using it to access this account through the regulations of financial institutions, Treating this account as an owner by making electronic transfers to oneself or others. And he could open a new account with the hope of that account in his name, After accessing the account, the aggressor can also change the password for accessing it so that the real account holder is denied access or transaction.

b- Submission of counterfeit requests:

The aggressor exploits the data seized, treats it as its owner, fills out forms for obtaining goods and services using such data, or the identity theft uses it to apply for a loan, leaving the real identity holder accountable for debts that have not benefited from them.

The aggressor may also request a cheque book in the name of the customer with the financial identity of a bank account and use it to write cheques without balance, thus placing the client with the financial identity in legal trouble for fraud offences.

c- The offence of publication and trafficking:

Publishing is intended to broadcast and broadcast information and financial data so that it is presented to everyone. It is also the process of broadcasting and transmitting information and data from one person to another without the permission of its real owner for the purpose of profit or damage.

We note that the publication here is a criminal act that is intentional and is intended to damage others expressly, and that it also works to publish financial identity data and increases the speed of obtaining them faster than it expands the extent of harm to others during the illicit use process.

The process of publication is to place the financial identity data for illegal access by all. This data and information is personal and contains secrets kept in private places, which the customer wants to keep confidential.

The assault is therefore not achieved if such information and data are available to all and are accessed by a person who is not allowed to access such information or data and is unauthorized access by any means.

Redissemination is also considered an offence punishable by law, with the redissemination of information that is unlawful or harmful to others. An aggressor who finds and redisseminates financial information is harmful to others.

Section II: Fraudulent transaction of financial identity data

This offence consists of the unlawful use of another personal identity intended either for the purpose of utilizing the status of that identity, i.e. the victim's identity or to conceal the identity of the offender to facilitate the commission of other crimes.

This crime is the use by a person of another person's identity to benefit from, for example, his reputation, funds or powers through information offence may result in the attrition of the victim's bank balance or the withdrawal of credit cards and debit cards, and the criminal often changes the victim's mailing address to his address in order to receive the invoices and requirements himself[1].

This offence is considered to be one of the most serious offences threatening private life and the right to privacy. For this purpose, the laws provide for legalcriminalties of imprisonment and fines.

The criminal conduct in this offence is to deceive the aggressor by exploiting and assuming the assumed financial identity. Article 247 stipulates that: "Anyone who impersonates himself in an official document for submitting to the authorities a name other than his own shall be liable to a fine of 500 to 5000 dinars." Article 249 states: "Anyone who impersonates another person during circumstances leading to the imposition of a judgement in the case law shall be sentenced to one to 5 years' imprisonment and a fine ranging from 100000 to 500000 dinars."

Although these materials do not speak of financial identity, they criminalize the abuse of the client's status, whether his private life, data or financial information, which may be used to prejudice him and involve him in legal problems with the financial institutions and business companies he deals with.

Conclusion:

At the conclusion of this study, it is clear that the financial identity data environment is subject to many risks. within financial institutions and business enterprises with which people interact, Or by offenders outside,

[1] Mohamed Khalifa, Criminal Protection of Computer Data in Algerian Legislation, New University House, Alexandria, 2007,p47.

and we tried to define the concept of financial identity theft. This is how we define financial identity as the subject of this crime, and in the end we have addressed the most important forms of theft as financial identity.

The right to protect financial identity from theft and to exploit its data to the detriment of the client is the requirement of everyone, especially the State, to enact laws to combat such attacks and to ensure legal protection of the privacy of financial information.

Results:

- In order to expand the availability of convenience for consumers and customers to conduct their transactions and access financial services, countries, especially in the field of financial institutions, have focused on exercising the privacy of financial identity data, and not being exposed to it, but on determining how to treat it with great confidentiality.

- Financial identity theft is a wide range of crimes that go beyond the theft of credit cards or the impersonation of a loan application. It is any assault using financial identity data at the level of financial and commercial transactions that do significant harm not only to the client but also to other parties such as financial institutions and commercial companies.

- Although there is no special law protecting financial identity data from attacks that may occur, there are a number of laws that provide the necessary protection and broadly prohibit any infringement on the privacy or disclosure of financial information to all, and its exploitation by illegal means.

- There are many risks to the integrity and security of financial identity data, and the stability of digital and commercial transactions performed by the client based on the financial information he has, in order to that the legislative and technical efforts in protecting such data are combined as an essential part of their business, namely the identification of strong policies and procedures for the security of financial identity data.

- Whoever triggered the theft of financial identity is what the aggressor is after, for example. potential cases brought by other parties dealing with the client whose data has been compromised, Restoring or repairing hacked systems costing financial costs s reputation and lack of confidence in the handling of financial identity until data is recovered, as well as financial losses and psychological damage to the dealer.

Recommendations:

- The traditional provisions of thecriminal Code are applied to certain offences infringing on financial identity data and the right to financial privacy of the client But there are crimes that require new legal provisions to govern their constituent criminal conduct, Such as theft of financial identity, these offences, which target financial statements relating to a person's financial position, It requires special explanatory legal treatment, and the legislator must put in place integrated legal protection through the law's texts.

- The customer must not share his financial statements with anyone who requests them on the phone, email or any other means or disclose them to the public only after confirmation of the authenticity of the requesting entity and whether it is a government body or financial institution dealt with by the identity holder, Also know the purpose of requesting this financial information and what will be used.

- Financial institutions and business companies with which people deal must ensure the confidentiality of documents, invoices, bank accounts, credit cards, periodic verification of the authenticity of their financial transactions, contact the owner of the financial identity and alert him of any infringements or abuses to which his financial identity data may be exposed.

- Customers, financial institutions and commercial companies must use computer protective software, continuously update them, provide them with antivirus software, and change passwords periodically, to protect these devices from hacking.

Reference

- **Book:**
- Alaa al-Tamimi, Legal Organization of the Online Bank, New University House, Alexandria, 2012.
- Ali Jamaluddin Awad, Banking Operations from Legal Point of View, Edition3, Arab Renaissance Publishing and Distribution House, Cairo, 2000.
- Marwa Zayn al-Abidin Saleh, International Legal Protection of Personal Data Online between International Convention Law and National Law, Center for Arab Studies, Egypt, 2016.
- Mohammed Amin Ahmed Al Shawabneh, Computer and Internet Crime, Edition1, Culture Publishing House, Jordan, 2004.
- Mohamed Khalifa, Criminal Protection of Computer Data in Algerian Legislation, New University House, Alexandria, 2007
- Nhla Abdelkader Al-Momani, Information Crime, Edition 2, Culture Publishing and Distribution House, Jordan, 2010.

- **Article:**
- David Bainbridge, Hacking (The Unauthorised Access of Computer Systems) - the Legal Implications -, The Modern Law Review, Volume 52, Issue 2,March 1989.
- Mona Turki Al-Mousawi, Information Privacy and its Importance and Risks of Modern Technologies, Baghdad College of Economic Sciences Journal, Special Issue, Baghdad, 2013.
- Naila Adel Mohamed Farid Qura, Economic Computer Crimes - Theoretical and Applied Study -, Edition 1, Halabi Rights Publications, Lebanon, 2005.
- Rafie Khader Saleh, Zina Sahib Curran, Restriction of Right to Information, Comparative Study, Al-Halabi Investigator Journal of Legal and Political Sciences, Issue 2, year 10, Baghdad, 2018.
- Suleiman bin Abdul Razek, Forms of Cyber Extortion Crimes and Their Motives and Psychological Implications, Security Research Journal, King Fahd Security College, vol. 27, No. 29, 2018.
- Zainab Star Jabbar Kazem Al-Lami, Civil Protection of Personal Data Online, Comparative Study, Misan Journal of Comparative Legal Studies, vol. 1, No. 5, Iraq.
- **Seminar article:**
- Ali Abdelkader Qahouji,criminal Protection of Electronic Data, Law, Computer and Internet Conference, May 1-3, 2000, Faculty of Sharia and Law, United Arab Emirates University, Abu Dhabi.
- Fashar Attallah, Confronting Information Crime in Algerian Legislation, Maghreb Forum on Law and Informatics, October 2009, Academy of Postgraduate Studies, Libya.
- **Legal texts:**
- Act No. 04-15 of 10 November 2004, containing thecriminal Code, Official Journal No. 71 of 10 November 2004.
- Act No. 15-04 of 01 February 2015, containing the General Rules on Electronic Signature and Certification, JR No. 06 of 10 February 2015.
- Act No. 18-07 of 10 June 2018 on the protection of natural persons in the handling of personal data, Official Journal No. 34 of 10 June 2018.