Pakistan Journal of Criminology
Vol. 16, No. 01, January—March 2024 (441-455)

Criminalization of Forgery of Electronic Payment Cards in Jordanian Legislation

Mohammad Nasr Khater[1]

Abstract

The article analyses the penal protection of electronic payment cards from forgery through a linguistic and virtual description of the notion of electronic payment cards. In addition to identifying the types of these cards, such as the credit card, the ATM card, and the debit card, the research also dealt with the offence of forgery of electronic payment cards by defining forgery and its forms, showing the jurisprudential difference in the application of the traditional forgery provisions in the Penal Law on Electronic Forgery, and also the Jordanian judiciary viewpoint regarding this topic through its judgments. The research concluded that the offence of forging electronic payment cards is based on the availability of three elements: the material element related to conduct based on changing the truth, the moral element, which is public and private intentions, and the necessity of the availability of the harm element. Also, the research came out with a recommendation that the Jordanian legislator should intervene in determining the bond or manuscript that may be exposed to forgery and determining its types and all its methods, in addition to developing texts for the definition of electronic payment cards, regulating its rules, and increasing its legal protection.

Keywords: Electronic Forgery; Credit Card; Payment Card; Cyber Crimes; Criminal Law.

Introduction

Bank cards are one of the most important forms of electronic payment worldwide, and hundreds of thousands of banks offer them to make huge profits and allow hundreds of millions of customers to buy their goods and services, and withdraw cash from ATMs that operate (24/24 hours), without the need to carry cash, it also provides them with the possibility to transact online and pay the financial obligations for this transaction through it, without the hassle of moving from one place to another (Bahri, 2020). Verbal forgery, worse than physical fraud, causes huge financial damages to companies and individuals and weakens financial institution faith. In the present era, electronic payment cards are used for automated teller machine purchases and sales.

[1] The author is a Lecturer in criminal law - Faculty of Law at the Applied Science Private University, Jordan. He can be reached at mo_khater@asu.edu.jo

Their widespread use has led to financial crimes that were previously unheard of, causing financial losses for individuals and institutions, whether through card forgery, card owner negligence, or other criminal methods. Forgery is one of the oldest and most common modern crimes. Credit cards, used in banking and as an alternative to cash-in purchases, have been susceptible to several fraudulent activities throughout the Arab world despite their recent adoption (Al-Asam, 2002).

Several security measures safeguard these documents from fabrication and aid police and technicians in their examination. These include the holograms, radioactive pictures, fine writing, bar code, metal wire, radioactive background, radioactive fibers and filaments applied to document paper, magnetic stripes, magnetic card signature strips, and others. Despite these new ways to protect documents, identification papers, and credit cards, computer technology (image scanners) and various types of colour photography have made them vulnerable to forgery and tampering, resulting in new crimes and criminal cases (Al-Asam, 2002).

Cybercrime and electronic forgery offences are prevented from being detected due to several factors, including the perpetrators' use of passwords or site passwords to prevent detection and evidence collection, thereby preventing expected inspections to search for evidence, as well as coding and encryption, and some utilise protection tactics to avoid being detected and arrested. (Al-Rahbani, 2020).

Literature Review

With the start of the third millennium, the world has entered an era suitable with the information and data revolution. This technological revolution has created new ways to conclude transactions for natural and legal entities that were unknown a few years ago. These methods have developed permanently, continuously, and rapidly.

To keep up with this speed of development, it was reasonable to consider how to interact among countries by encouraging and supporting trade and financial activities and integrating financial and economic systems and legislation. Monetary institutions and banks arose, and modern procedures were utilised to interact with individuals and institutions and exchange interests. Credit cards and their use in simplifying and speeding up the exchange of common interests between individuals and local or international financial institutions, as well as the spread of computer systems and automated banks to replace currencies and exchange orders (cheques), are recent methods.

Before 1950, American oil firms introduced credit card, and banks used advanced networks to swap interests. It was unsuccessful until the sixties, but financial progress in the eighties disseminated it broadly across Western Europe and America. The growth and circulation of credit cards locally, regionally, and globally has led to manipulation and fraud in some Arab countries and others. Millions were lost in America and other countries, including Arab ones. (Khayyat, 2002)

Forgery, theft, and alteration of electronic payment cards have begun to affect a broad percentage of people, and criminals will find more complex ways to implement their schemes, therefore they must be stopped by all accessible and possible measures. (Khayyat, 2002). The legislation for criminalising the forgery of the electronic signature in electronic payment cards had three directions: general texts to criminalise forgery in all its traditional and electronic forms, such as French and German law, and special texts for electronic forgery in general without distinguishing between the electronic signature and the secret number. Other electronic signatures, like the Egyptian legislator, and the third specifies a special text for counterfeiting electronic payment cards, like the Omani law. (Khattabi, 2020)

Even for the data recorded on electronic payment cards, Gant believes that jurisprudence considers them a bond or document, and changing the truth in this data is the physical element of forging. As this data can be seen with the naked eye, it may be read with a card reader and understood. A bond in informatics is any physical object, such as a disc or magnetic tape, that may support information, including electronic payment cards (Al-Qahwaji, 2010). Relying on invisible data processed electronically is a narrow interpretation of the document that prevents scientific progress and undermines confidence in electronic documents, especially as modern society and institutions increasingly rely on them (Khattabi, 2020).

Electronic Payment Card Notion

Electronic payment cards have become popular among dealers because they are more effective, easy to carry and use, secure, and allow dealers to trade locally and globally without keeping large amounts of cash. They are also widely used in the commercial environment and have become one of the main activities of banks and financial institutions (Al-Anazi, 2015).

What is an Electronic Payment Cards?

There are multiple definitions of electronic payment cards, and these definitions will be addressed linguistically, jurisprudentially, and legally as follows:

The linguistic definition, according to "Lisan Al-Arab Dictionary" (as Abi Al-Arabi and others mentioned, the "paper card" is a small patch whose amounts according to the value on which it is based, so if it is in kind, then it is evaluated by weight or a number, and if it is a commodity, then it is evaluated by value), then the word "card-bitakah" It is an eloquent Arabic word, meaning the small patch or paper, and this is the origin of the card, then it developed and became made of plastic to ensure that the information is not damaged or changed quickly, and is used at present in its eloquent linguistic sense, except that it is concerned with what is added to it, so it is said that a debit card, a credit card, or a personal card and thus, its meaning is determined by what is added to it. (Al-Duwaikat and Al-Shibli, 2013).

The jurisprudence definition is different as it states "a modern payment and withdrawal tool, the card transfers traditional cash between the accounts of the parties dealing with it through computerised networks and provides many advantages according to card type, value, and credit duration, by the contract between the parties (Al-Saqqa, 2007). It is also a triple-party or quadruple-party card with independent original obligations and its legal system based on the contract between the cardholder and the issuer (Abd Alhakam, 2003).

These definitions of electronic payment cards are based on credit, which is their basic essence, due to several factors, including the trust between the issuer and the holder and the sufficient time between providing and recovering the means of fulfillment (Al-Anazi, 2015).

The Jordanian legislation does not define electronic payment cards, as some believe the legislator should intervene in the regulation of its provisions, while others believe the opposite, due to the rapid development of these cards and legislation cannot keep up with that. Jurists have defined it based on different criteria, including function and length, thickness, and material of manufacture, bearing in mind that electronic payment cards have different types, each differing from the other in terms of the issuer, credit limits, and function performed. (Abu Issa, 2019).

Types of Electronic Payment Cards

a. Credit Card:

One of the most important types of e-payment or fulfillment cards, the possession of which depends on a special contract between the issuer and the customer, is a tool for both fulfillment and credit, allowing the card holder to obtain goods and services without immediate payment. The card does not require the customer to have a balance in his account with the issuing bank, so the due amounts are debited from the account (Al-Anazi, 2015).

b. ATM Card (Automated Teller Machine Card):

ATM cards allow the holder to withdraw cash from his account to an agreed maximum limit per day, i.e., there is a cap for ATM withdrawals, and the withdrawn amount is recorded as a debit to the customer's account directly. This card does not perform a credit function, so the customer can only withdraw cash from his balance (Abu Issa, 2019).

c. Debit Card

In addition to ATM redemption, this card allows the holder to pay for goods and services at some shops that accept the card as a payment instrument under an agreement from the issuer by transferring the price from the customer's account to the merchant's account. The card is used in place of a cheque to pay for goods and services at the merchant's premises (Kalou, 2015).

Banking institutions now issue cards with the benefit of ATM withdrawals and fulfillment, allowing the holder to withdraw cash from the bank's outlets, whether internal or external, with the amount immediately deducted from his account. The card can also be used to make purchases with the holder's money (Al-Hiti, 2009). Many types of cards perform the same functions as the previous types in different ways, and with recent evolution, their functions and advantages have changed, but they still perform the same basic tasks as the aforementioned cards, such as online shopping cards or smart cards.

In the Electronic Crimes Law No. 17 of 2023, the Jordanian legislator confronted the attack on information and data of electronic payment cards through the text of Article (8), which stipulates that: A shall be punished by imprisonment for not less than one year and not to exceed three years and a fine of not less than (2500). (Two thousand five hundred dinars and not more than (10,000) ten thousand dinars for each of:

> 1: He intentionally obtained data or information related to electronic payment methods or in the implementation of financial or electronic banking transactions through the computer network, information technology, or information system, or used or published any of this data.
>
> 2. Invent, create, develop, or design any information technology means, information programme, or programmeming command with the intention of facilitating obtaining the data stipulated in Clause (1) of this paragraph.
>
> 3: Before dealing with forged, imitated, or copied cards or other electronic payment methods, or data on electronic payment methods that were illegally seized, be aware of their illegality.

If the data and information are used to obtain the money of others or to benefit from the services they provide and the use does not lead to a result, the penalty shall be imprisonment for not less than two years and not more than three years and a fine of not less than (5,000) five thousand dinars and not more than (15,000). Fifteen thousand dinars.

If the actions stipulated in paragraphs (a) and (b) of this article result in seizing for himself or others property owned by others or benefiting from the services it provides, then the penalty shall be imprisonment for three years and a fine of not less than (10,000) ten thousand dinars. Not more than (20,000) twenty thousand dinars.

Despite the Jordanian legislator's desire to protect electronic payment cards and the latest cybercrime law's conformance with international standards, it did not include language on card forgery.

Offence of Forgery of Electronic Payment Cards.

Credit card offences are complicated, complex, and sophisticated, and many offences are difficult to limit because their methods are varied, the perpetrators are different, and their classification is difficult. They are modern emerging and technical offences that change daily, so they cannot be limited (Dababneh, 2014).

To understand the offense of electronic payment card forgery, it will be divided as follows:

A. The Concept of the Offence of Forgery of Electronic Payment Cards:

To understand electronic payment card forgery, it is necessary to define the offence, explain its elements and forms, and clarify how the Penal Law applies to it, as follows:

i. Definition of Electronic Forgery

Article (260) of Jordan's Penal Law No. (16) of (1960) defines forgery as: "An artificial misrepresentation of the truth in facts and data that will be intended to be proven by bond or manuscript or official information system data that is invoked as a result, or may result, of material, moral or social harm". Jordanian law did not define electronic forgery, so some legal definitions were as follows: "Any change in the facts reflected in the computer output, whether in the paper output written, printed by the printer or drawn with a drawing, the information document is written in Arabic, archived in a supported software, and copied on a CD, provided that the information document has the effect of establishing (Hejazi, 2002).

Others defined it as: "falsification of documents and data on a computer, and falsification of information so that alternative information is provided instead of

actual information", as the offense of forgery generally targets documents and data, particularly those relating to financial entitlements, bank deposits, accounts and results of budgets, payment instructions, sales lists, electronic transfer systems for funds and bank deposits (Al-Nosour, 2021).

ii. Electronic Forgery Elements

The material element of the forgery offence is the misrepresentation or alteration of the truth in one of the methods the law provides exclusively. The change does not need to be complete, i.e., the replacement of all data with others that contradict the truth, and it can be partial or relative. Documents are often susceptible to offence. The moral element is criminal intent (Al-Jubouri, 2017).

The general criminal intent required to forge electronic payment cards is not enough; there must also be a special criminal intent due to the offender's lack of knowledge of the elements of forgery or that his will tends to alter the truth. Above all, his will must be directed towards using the forged card for the purpose for which it was forged (Al-Anazi, 2015; Abu Issa. & Al Shibli, 2022).

For forgery to be committed, the harm must occur, but it does not have to occur if the possibility of it occurring is sufficient. The material or moral harms are equal, as the harm is material if it affects the person's financial liability and moral if it relates to the moral entity of the person, his honour, and his capacity (Ahmad, 2005). The bond or document is important in the context of forgery because it is a container containing the truth subject to manipulation and alteration. Altering the truth alone is not enough to commit forgery unless the alteration is on or within a document (Al-Hiti, 2009).

iii. Forms of Electronic Payment Card Forgery

This is done either by fabricating a complete plastic card, starting with imitation of printing, engravings, and logos on the plastic, wrapping the card, pasting the hologram, pasting the magnetic stripe and signature tape, making the magnetic strip either by copy or encryption, and then making the prominent printing with the illegally obtained information. The card is traded and used in purchases, or the fully processed cards are stolen (Al-Duwaikat and Al-Shibli, 2013).

The offender can invest the body of a genuine card with its logos and data obtained by any method, such as theft or possession of an expired card, but its theft will hinder its use, as it is promptly reported, which leads to the issuer's circular to all card use ports to not accept the card, making the offender's use of the card impossible (Al-Hiti, 2009).

iv. Use of Forged Electronic Payment Cards

The offence is committed in the form of forged use, where the person who stole or found the card signs the purchase invoice by imitating the signature pattern on the back of the card. Legislation has been keen to criminalize the use of forged documents and made this offence separate from the act of forgery itself. The offence of using a forged document refers to the act of using a counterfeit credit card to purchase goods or services from the supplier merchant. Furthermore, punishment for the use of a forged document is applicable even if the user is not the forger himself. (Mohamadi, 2015).

It is also required to deceive the merchant or the automated device, which means that the perpetrator successfully manipulates the withdrawal or fulfill by using forged data. In addition to the criminal intent to deliberately change the truth in the document, and the card user is aware that it is forged and willingly chooses to use it. Thus, all the elements of the crime are fulfilled, and the focus of the offence is directed toward the forged document, which applies to electronic payment cards (Mahioubi, 2016).

The elements of the offence of using a forged document are manifested in the act of the accused in possession of the forged document in the realm of circulation and use, despite being aware of its forgery. Here, the elements of the offence of using a forged document are fulfilled. By applying this to the use of a counterfeit credit card to settle some purchase with a merchant, once the counterfeit card has been presented to an authorized merchant recognized by the issuer to settle the purchase, the material element of the offense is the act of use. In addition, the criminal intent (the moral element) is present because the person presenting it to the merchant is aware of the forgery and relies on the forged data to influence the merchant to accept it for payment, thus, the latter obtained a benefit from its use and causing harm to the genuine cardholder bearer of the act (Mohamadi, 2015).

Analysing the offences of forging electronic payment cards and using a forged document, it turns out that they are interrelated offences, as the commission of the second offence must come after the completion of the first offence, and the same perpetrator is often involved in both crimes.

Many legislations devoted considerable attention to cybercrime and criminalized acts that constitute an infringement of the electronic environment by special legislative texts regulating their provisions, however, some legislations did not establish specific provisions to criminalize such offences, but have merely applied the traditional provisions governing the provisions of traditional forgery, including Jordanian legislation. It has been disputed to the extent to which traditional provisions can be applied to the offence of electronic forgery as follows:

The Contrary Trend to the Application of Traditional Provisions to the Offences of Forgery of Electronic Payment Cards

Proponents of this trend believe that the provisions of traditional forgery cannot be applied to the forgery of payment cards because forgery according to the traditional provisions must occur on a document, or as contained in Article (260) of the Penal Law (Plea by bond or manuscript), and this document must be in writing, while the cards are not documents, and therefore the magnetic stripe or electronic chip is not a document, and therefore provisions regarding forgery cannot be applied to the facts alteration in the data and information stored on the card (Abu Issa, 2019).

This is evident from the fact that the two main reasons for not applying the traditional texts are the rigidity of the criminal text, which makes it difficult to interpret on a large scale, due to the absence of any reference to new forms emerging from documents, so long as there is a link between document and writing, which often has a paper connotation, and the relationship between committing the offence of forgery and the requirement of a document with an evidentiary value requires reference to the laws of evidence and how they regulate the written evidence (Al-Jubouri, 2017). The proponents of this trend have established special legislation criminalizing the forgery of electronic payment cards such as Moroccan, Syrian, Omani, Emirati, and Qatari legislators.

Omani Legislation

In the Sultanate of Oman, Law No. (12) Of (2011) was issued to combat cybercrimes. Article (2) of this law stipulated the repeal of the provisions in the second section (bis) of the seventh Title of the Omani Penal Law, which previously applied to the forgery of electronic payment cards before the issuance of this law. Furthermore, any provisions contradicting or conflicting with the attached law were also repealed. The Omani legislator introduced the term "financial card" to refer to payment cards and he specified its types. The definition of financial cards was provided in Article (1) of the same law, stating that "they are "A concrete electronic intermediary used in electronic withdrawal, deposit, or payment operations through the use of information networks or information technology means, such as credit cards and smart cards, it does not include communication cards and prepaid electronic service cards."

Payment cards are explicitly mentioned in the same law in Article (28), which states: "A term of imprisonment of not less than one month and not more than six months and a fine of not less than five hundred Omani Riyals and not more than (1,000) Omani Riyals or one of these two penalties shall be imposed on anyone who forges financial card by any means or forgery or manufactures or counterfeits

devices or materials that facilitate forgery or obtains data of a financial card, using it, offering it to others, facilitating its obtaining, illegally accessing financial card numbers or data using information networks or information technology, or accepting a forged financial card with knowledge of its forgery."

The Omani legislator was criticized for leaving the punishment to the judge's discretion between the two penalties, imprisonment and a fine. Therefore, the judge has only the authority to impose either a fine or imprisonment exclusively (Mahioubi, 2016).

According to Royal Decree No. (8) of (2018) promulgating the National Payment Systems Law, credit cards were explicitly mentioned in one of its articles as a payment instrument, whereas credit cards were specified in Article (1) as: "a tangible or intangible instrument that enables a person to obtain funds, goods, and services or to perform payment transactions and financial transfers. This includes, for example, cheques and money transfers made through ATMs, points of sale, the Internet or telephone and payment cards such as debit cards, credit cards, smart cards and electronic money storage cards."

In Article (57) of the tenth chapter concerning penalties, it states the offence of forgery of payment instruments as follows: "Anyone who imitates or forges any payment instrument, or acquires, uses, or attempts to use a counterfeit or forged payment instrument with knowledge thereof, shall be punished with imprisonment for a period not less than one year and not exceeding five years, and a fine of not less than (10,000) Omani Riyals and not exceeding (50,000) Omani Riyals. The same punishment shall apply to anyone who forges information and data contained in transactions conducted or executed in the system, or who uses any means to access such information and data without authorization."

UAE Legislation

The UAE legislature has issued Federal Law No. (34) Of (2021), which is a specialized law addressing the combating of rumours and cybercrimes. This law defines the actions that constitute an assault on electronic payment methods and specifies the corresponding penalties under Article (15). The article stipulates the following:

"Anyone who forges, imitates, or copies a credit card, debit card, or any other electronic payment instrument, or unlawfully obtains its data or information, using information technology means or information systems, shall be subject to imprisonment and a fine not less than (AED 200,000) (two hundred thousand Emirati dirhams) and not exceeding (AED 2,000,000) (two million Emirati dirhams), or one of these two penalties. The same penalty shall be imposed on:

1. Manufacturing or designing any information technology means or software program to facilitate any of the acts mentioned in the first paragraph of this article.
2. Using a credit card, electronic card, debit card, or any other electronic payment method, with its data or information, without permission, to obtain, for himself or for others, funds or property owned by others or benefiting from services provided by others.
3. Accepting and dealing with forged, imitated, copied, or other illicitly obtained electronic payment cards or data of electronic payment means, with knowledge of their illegality.

Qatari Legislation

The Qatari legislation includes provisions with deterrent penalties against perpetrators of computer and electronic payment offences through the issuance of Law No. (14) Of (2014) on Combating Cyber Crimes. In Article (1), the law defines the electronic transaction card as "an electronic card that contains a magnetic strip, smart chip, or any other information technology means, which includes electronic data or information, and is issued by the licensee".

Article (12) criminalizes the falsification of electronic transaction cards, which stipulates that: "Anyone who commits any of the following acts shall be liable to a term of up to three years imprisonment and a fine not exceeding two hundred thousand Riyals (200,000), or either of these penalties:

1. Use, obtain, or unlawfully access electronic transaction card numbers or data through the information network or any means of information technology.
2. Forge an electronic transaction card by any means.
3. Manufacture or possess, without authorization, devices or materials used in the production or forgery of electronic transaction cards.
4. Use or facilitate the use of a forged electronic transaction card, knowing it to be forged.
5. Accept invalid, forged, or stolen electronic transaction cards, knowing them to be so.

It is noteworthy that the Qatari legislator has not only criminalized the forgery of electronic transaction cards and the use of forged cards but has addressed more than that. The law stipulates punishment for anyone facilitating the use of a forged card and for those who manufacture and possess devices used in forgery. Thus, the mere act of manufacturing and possessing such devices constitutes a crime punishable by law. This indicates that the law encompasses all issues related to

electronic transaction cards that may contribute, in one way or another, to the occurrence of forgery offences.

The Supported Trend to the Application of Traditional Provisions to the Offences of Forgery of Electronic Payment Cards:

Proponents of this trend argue that the traditional Penal Law can be applied to the offence of forging electronic payment cards because there is no difference between a copied or abridged document and electronic information can be used as proof, especially since electronic recording of information is a form of documentation, there is a relationship between the penalty of forgery and evidentiary procedures, and there is a link between the physical and moral methods of forgery and the means of committing electronic forgery, which can be legally identified by placing forged signatures., either through the inputs of the computerized system or through its outputs, as regards the forms of alteration of documents, seals or signatures, it is possible to modifying them electronically, since a computer is a means of receiving and processing information and data electronically.as regards the forms of alteration of documents, seals or signatures, it is possible to modifying them electronically, since a computer is a means of receiving and processing information and data electronically (Al-Aridi, 2012).

The Jordanian judiciary has applied the Penal Law to the offence of forging electronic payment cards, as shown in Articles (260-265) of the Public Trust Offences Section.

Challenges in investigating and prosecuting electronic payment card forgery:

Many problems and obstacles affect the investigation process, resulting in the investigator's loss of confidence in himself and his performance, society's loss of confidence in law enforcement agencies that cannot protect him from these crimes and prosecute their perpetrators, and the criminal himself, He feels that the security authorities cannot uncover his matter and that those in charge of combating and investigating do not match his expertise and knowledge, which gives him tremendous confidence in committing more of these crimes that may affect society (Abu Issa, & Khater, 2023). Among the most important obstacles facing those in charge of combating computer and Internet crimes are below.

a. Legislative challenges

The lack of incriminating texts against computer and Internet crime criminals means that the phenomenon will worsen and make treatment more difficult than expected, especially since all transactions and procedures will be

electronic and the judiciary does not rely on the investigation bodies' evidence upon inspection. Computer crime perpetrators are arrested and investigated because there are no rules and consequences that define illegal activity (Al-Halabi, 2011; Khater, & Abu Issa, & Alwerikat, 2023).

The Code of Criminal Procedure lacks many of the legal texts necessary to confront the special nature of computer and Internet crimes, as follows:

First: No rules govern the inspection of computers connected abroad (Issa, & Alkhseilat, 2022).

Second: The need to adapt criminal proof theory to moral evidence. (Al-Halabi, 2011)

Third: The Code of Criminal Procedure did not specify how to handle a computer owner or user who refuses to give the password or installs a virus to disrupt the investigation and erase evidence of his crime (Al-Halabi, 2011).

b. Technological challenges

Technological hurdles relating to the crime hinder investigators. The absence of visual evidence that can be read and understood, as well as the difficulty of accessing the evidence because it is protected by technical means, such as passwords around their sites or encrypting it, To prevent access, viewing, or reproduction (Abu Issa, Ismail, & Aamar, 2019).

The speed at which evidence can be erased or destroyed hinders crime investigations. Given the large volume of information and data that must be examined and the possibility that it is out of date, the perpetrator can erase or destroy evidence against him quickly, preventing the authorities from detecting the crime. The state's territory and certain concerned parties' ignorance of Internet crime components (Al-Halabi, 2011).

Conclusion & Recommendations

In summary, forging electronic payment cards threatens people and public confidence online, and after studying and analysing the research topic, the following conclusions and recommendations can be drawn:

- The Results:

- Credit cards, ATM cards, and debit cards are the most common electronic payment cards.
- The crime of electronic forgery involves two elements: material, which involves altering the facts, and moral, which involves public and private intentions and the potential for harm.

- Forgery of electronic payment cards can be done in two ways: complete forgery by fabricating the card's physical body and storing data, or partial forgery by adding or deleting data.
- The Jordanian judiciary has applied traditional Penal Law provisions to the offence of forging electronic payment cards, as outlined in the Public Trust Offences Section, Articles (260-265), as shown by verdicts.
- Jordanian legislators should develop texts defining, regulating, and protecting electronic payment cards.
- Jordanian legislators must address forgery risk in bonds and manuscripts, including types, forms, and procedures.

References

Abd Alhakam, S. (2003). *Credit card criminal protection*. Cairo: Dar Al-Nahda Al-Arabiya.

Abu Issa, H. & Khater, M. (2023). Distance Indecent Assault Crime in Jordanian Law Perspective. *Pakistan Journal of Criminology*, Vol.15, Issue 1, 125-138.

Abu Issa, H. (2019). *Information technology crime*. Amman: Dar wael.

Abu Issa, H. and Al Shibli, M. (2022). The Avenge as a Motive of Homicide Crimes in Jordan for the Period (2017-2021). *Pakistan Journal of Criminology*, Vol.14, No.1, 112-127.

Abu Issa, H., Ismail, M., & Aamar, O. (2019). Unauthorized access crime in Jordanian law (comparative study). *Digital Investigation*, 28, pp. 104-111.

Abu Khalaf, F. (2007). *Criminal Protection for Credit Cards* (Master Thesis, Naif Arab University for Security Sciences, Riyadh).

Ahmad, I. (2005). *Civil and criminal legislative protection for electronic payment cards*. Alexandria: Dar Al-Jamaia.

Al-Anazi, M. (2015). Criminal Protection of Electronic Payment Cards from Forgery. *The Arab Journal for Security Studies and Training*, Volume 31, Issue 62.

Al-Aridi, F. (2012). The Crime of Electronic Forgery. *Kufa Journal*, Issue 13.

Al-Asam, O. (2002). *The most widely used credit cards in Arab countries.* a paper presented to the proceedings of the Credit Card Fraud Symposium, Naif Arab Academy for Security Sciences, Riyadh.

Al-Duwaikat, M. and Al-Shibli. H. (2013). Forms of Credit Card Fraud and Forgery. *The Arab Journal for Security Studies and Training*, Volume 29, Issue 58.

Al-Halabi, K. (2011). *Procedures of Investigation in cybercrimes.* Amman: Dar Al-Thaqafa.

Alhiti, M. (2009). *Criminal protection for magnetic credit cards*. Cairo: Dar Alkotob Alqanonia.

Al-Jubouri, O. (2017). *The Crime of Electronic Forgery in Jordanian Legislation* (Master Thesis, Middle East University, Amman).

Al-Nosour, M. (2021). Material and Moral Methods of Forgery by Application to the Egyptian and Jordanian. *The Legal Journal* Volume 9, Issue 13.

Al-Qahwaji, A (2010). *Criminal Protection of Computer Programmes*. Alexandria: New University House.

Al-Rahbani, A. (2020). *Cybercrime and its risks*, Amman: Dar Althaqafa.

Alsaqa, S. (2007). *Forensic and security protection for credit cards.* Alexandria: Dar Al-Jamaa Aljadeeda.

Bahri, A (2020). The effectiveness of using electronic payment cards within the requirements of e-commerce orientation. *Journal of Economic, Facilitation and Commercial Sciences.* Volume 13, Issue 3.

Dababneh, S. (2014). Credit Card Crimes, A Sociological View. *Journal of Banking and Financial Studies*, Issue 3.

Hejazi, A. (2002). *Criminal evidence and forgery in computer and Internet crimes.* Cairo: Dar Alkotob Alqanonia.

Issa, H.A., & Alkhseilat, A. (2022). The cyber espionage crimes in the Jordanian law. International *Journal of Electronic Security and Digital Forensics*, 14 (2), pp. 111-123.

Kalou, H. (2015). Electronic Payment Card in Algerian Law. *Journal of Human Sciences*, , Volume A, Issue 44.

Khater, M., Abu Issa, H., & Alwerikat, N. (2023). The Mother Killing of her Newborn to Avoid Disgrace under Jordanian Law. *Pakistan Journal of Criminology*, 15 (4), pp. 21-27.

Khattabi, F. (2020). Forgery of Electronic Signatures in Credit Cards, *Algerian Journal of Human Security*, Volume 5, Issue 2, 649-668.

Khayyat, M. (2002). *credit card fraud operations.* paper presented to the proceedings of the credit card fraud symposium, Naif Arab Academy for Security Sciences, Riyadh.

Mahioubi, F. (2016). *Electronic payment card crimes.* (Master Thesis, Mohammad Khaidar University, Baskra).

Mohamadi, A. (2015). Criminal responsibility for illegal use the credit card. *Journal of North African Economies.* Issue 13.