International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 432-443 www.ijaem.net ISSN: 2395-5252

The Payment Service Providers in Palestine: With Special Reference to the Issues of Security and Confidentiality in E-Transaction

Yahya Yousef Falah
Assistant professor, Faculty of law, An-Najah University, Palestine

Submitted: 01-03-2021 Revised: 09-03-2021 Accepted: 12-03-2021

ABSTRACT: The biggest beneficiaries from the development of the Internet have been the banks. The banks have started offering their services by using the Internet, and likewise, many individuals have become dependent on modern techniques for paying the price of goods electronically. In order to make it easier for users, the banks have started to use the Internet in offering their services. Many people now use credit cards to pay for goods and services. They avoid carrying paper money which is often exposed to theft or loss. Therefore, the payment service providers play an essential role in pay the price of goods and services in e-transactions. This paper will examine the role of payment service providers in e-transactions in Palestine. In addition, this paper seeks to clarify the issues of security and confidentiality of the users during of the payment process in e-transactions. This study mainly used the analytical and library research to examine the issues of payment security and privacy in e-transaction. The laws of Palestine are used in this study to clarify the legal positions on the relevant issues above. It is found from this study that the issues of security and privacy require the legislations which regulate the legal matters of payment service providers in Palestine such as the security of the websites against any risks including viruses and hackers. Moreover, the banks are obliged to protect the privacy of the users when they open an account and provide the bank with their personal information. On the other hand, the users need information and some experience in using internet banking and maintain their security during payment and money transfers between many accounts. Likewise, the users need information about protecting their information when accessing the website of the bank including protecting their passwords and usernames and the secret number of their credit cards, besides of protecting their computers against any viruses. Therefore, the cooperation between the government, legislators, banks and the individuals is necessary to overcome such problems and to develop e-banking in Palestine and e-commerce in general. The benefit of this paper is to propose some recommendations to develop the Palestinian laws in order to address the issues of payment security and privacy which will contribute in the development of e-commerce in Palestine.

KEYWORDS: PaymentService Provider, Payment Security, Electronic Signature, the Privacy.

I. INTRODUCTION

The biggestbeneficiaries from the development of the Internet have been the banks. The banks have started offering their services by using the Internet, and likewise, many individuals have become dependent on modern techniques for paying the price of goods electronically.

In order to make it easier for users, the banks have started to use the Internet in offering their services. To this end, they have created sites on the Internet, enabling their clients to manage their accounts and do a variety of banking operations electronically from the place of their work or residence. The banks have also enabled their clients to pay the prices of goods and services electronically. Many people now use credit cards to pay for goods and services. They avoid carrying paper money which is often exposed to theft or loss. Therefore, the payment service providers play an essential role in pay the price of goods and services in e-transactions.

Palestinians are comfortable in using the Internet for financial and banking services, and they are open to online transactions and payments. Regarding this, Palestinians are using many methods of payments in e-transactions and the highest percentage was payment by cash on delivery which was 86.5. In addition, the percentage of individuals aged 18 years and above in the Palestinian territory who used payment by

the credit card through the Internet was 15.2 % in 2019. On the other hand, the percentage of using a direct debit card or electronic banking transfaring through the Internet was 7.5 % in 2019. However, the percentage decreased when using the payment services through the Internet which was 3.7% in 2019. Finally, the method of payment through account with mobile was the lowest percentage with 1.9%[1].These statistics reveal that the Palestinians used many methods of payments in e-transactions, and they preferred the cash payment to avoid the problems which may occur in case of using the otherpayments methods. In fact, the electronic payment creates many concerns to the consumers especially the security and privacy threats which need a high level of legal and technology solutions.

As a rule, security and privacy are the main problem that affect the wish of people in managing their banking accounts and financial operations electronically. Furthermore, a lack of knowledge about how to manage the financial operations electronically is another problem which reduces the percentage of using e-banking. In fact, all these problems have a substantial effect on the development of e-banking in Palestine. Therefore, the cooperation between the government, legislators, banks and the individuals is necessary to overcome such problems and to develop e-banking and payment service providers in Palestine and e-commerce in general.

In fact, this study attempts to examine and analyse the legal issues related to payment service providers, especially in e-transaction. In addition, there are many concerns about using e-banking services such as privacy and security. Therefore, the researcher will discuss the issues of e-banking and online payment that protect individuals during payments in e-transaction in Palestine. In addition, this study is important as it examines the Palestinian legislations which regulate the issues of security and privacy in e-transactions.

II. PAYMENT SERVICEPROVIDER

The electronic payment service provider is defined in the Instructions No. 1/2018 regarding of licensing the payment service companies: "The company that is licensed from the Monetary Authority to introducing the payment service by the electronic means"[2]. In addition, the Instructions No. 3/2020 regarding of organizing the relation of payment service companies with the users define the payment service as: "The licensed company from the Monetary Authority to introducing the payment services"[3]. It can be concluded from these definitions that the payment service provider plays an essential role in e-transactions especially in pay the price of goods and services. Therefore, the Instructions oblige the payment service provider in obtaining the license from the Monetary Authority before starting his works. In general, the license is an important requirement on the payment service provider to grants the Palestinian Monetary Authority the power to control and monitor their works in the purpose of providing a high level of protection to the users during the electronic payments**.**

The traditional payment service providers include the issuing of the credit card, and the "acquiring" bank, which is used by the merchant or seller, card networks and payment processors which process payments between merchants and acquiring banks [4].

Payment charging is controlled by the payment service provider, which could be a network operator, financial institution, a credit card company, or an independent payment vendor [5]. In addition, the payment service providers can work by themselves or depend on a third party. Therefore, the Instructions No. 1/2018 regarding of licensing the payment service companies stipulate that: "The payment service provider is allowed to outsource any of his works to a third party in terms of prior written approval from the Monetary Authority" [6]. It can be concluded from this article that the payment service provider can do his works by himself or he can rely on a third party, and it is obliged to obtain an approval from the Palestinian Monetary Authority in case of relaying his works on a third party.

In addition, the Palestinian Monetary Authority has the power to accept or reject the request of outsourcing according to article 14/2 of the Instructions No. 1/2018 regarding of licensing the payment service companies: "The Monetary Authority has a power to reject the request of outsourcing of the major operation prosses if it believes that outsourcing may affects on the quality of internal control, or if it affects on the ability of the Monetary Authority on its supervisory powers" [7]. It can be concluded that, the payment service provider does not have a full option in relaying on a third party , and this issue depends on the Monetary Authority which can reject outsourcing depending on the circumstances. Therefore, the payment service provider cannot rely on a third party if this affects on the internal works. As a result, this article is important to control the works of payment service provides and providing the payment services in the effective way to protect the user's data during the payment prosses.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 432-443 www.ijaem.net ISSN: 2395-5252

Furthermore, the Palestinian Monetary Authority regulates the instructions that allow the banks to outsource their operations with third party service providers according to the Presidential Decree No. 9/2010 regarding of Banking Law. The bank is obliged to put the full procedures on managing and controlling the outsourcing operations. In addition, the bank is obliged to obtain prior approval from the Monetary Authority for any management, renewal, or change of outsourcing [8].Likewise, the Instructions No. 5/2010 regarding of automated connectivity and outsourcing regulated the contractual terms between the banks and outsourcing service provider, and these contracts must be compliant with the Palestinian laws and Instructions [9].

In general, it allows the Palestinian Monetary Authority to create the regulations of outsourcing and monitor the application of these regulations by the banks to protect the rights of the users, as this authority is official. This authority can oblige the bank to follow the regulation, and it can apply some penalties on the bank if it did not follow these regulations. An example these penalties include withdrawing the permission of outsourcing, or not giving the bank the permission for outsourcing. In fact, these regulations are important to protect the rights of the consumers when they provide the bank with their information and the bank submit this information to the third party for outsourcing. Therefore, the security and privacy of the consumer is essential to issues and any problem resulting from outsourcing may affect the consumers.

In General, There Are Many Types of Payment Service Providers In E-Transactions such as:

Banks: The banks play an essential role in pay the price of goods and services especially in e-transactions. Therefore, many banks started in providing their services by the electronic means especially through the Internet. The Palestinian Presidential Decree No. 9/2010 regarding of Banking Law defines the electronic banking as: "Using the electronic means in the enforcement of bankingoperations"[10]. In fact, the electronic banks depend on the electronic means, and the electronic banks play an important role as a payment service provider in e-transactions.

Online Payment Service Provider: The Instructions No. 1/2018 regarding of licensing the payment service companies define the electronic payment service provider as: "The company that is licensed from the Monetary Authority to introducing the paymentservices by the electronic means"[11].

Payment Card Issuer: The card issuer is: "The cardholder's bank who issues the card and maintains the customer's accounts"[12]. Therefore, the card issuer plays an important role as a payment service provider in e-transactions.

III. ISSUES OF PAYMENT SECURITY

The banks are an important organization in the global market, and they play the main role in the payment process in e-transactions. However, the security issue is a concern to all parties who are involving in the payment process in e-transactions especially the seller and buyer.

E-banking leads to many concerns for businesses and individuals. In fact, businesses are concerned about security, so they do not offer online payment options, which might affect their customer base, as there are some customers who prefer to pay online. However, these customers are also concerned about the security of their information whenever they log into their respective online accounts [13].

As an example, there were 4,818 websites breached every month in 2018. In addition, every credit cards data was sold by almost $ 45 in the black market. In addition, the cyber criminals can obtain more than $2.2 million every month from only 10 stollen credit cards [14].

As a matter of fact, hackers attempted to breaking through the websites every day especially the bank's websites. In this case, the hackers attempt to steel the credit card's data due to the greediness in the benefits of these types of crimes as it is an easy way to collect a high sum of money in a short time. In addition, hackers exploit the weak experience of the users and the weakness of the websites security to execute their crimes. In fact, every user who has banking account is under the risk of having his information stolen. Therefore, the banks and payment service providers are obliged to adopt all the necessary procedures to prevent the attackers from breaking through their websites.

Online banking depends on the security of the transaction, which is an important consideration for the costumer. The confidence of customers with online banking depends on the degree of security. Banks are attempting to attract more customers by increasing the levels of confidence in their security measures. Basically, doing so, will guarantee increased customer adoption of online banking [15].In addition, the security and trust of the electronic payment is essential for e-commerce. Electronic banking and e-payment must adopt the sophisticated technology to build a strong security system [16].

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 432-443 www.ijaem.net ISSN: 2395-5252

For this reason, the Instructions No. 3/2020 regarding of the relation between payment services companies with the users stipulates in article 2: "These instructions aim to regulate the relation between the service provider with the users in the security and transparency way"[17]. In addition, these instructions oblige the payment service provider in article 3 to adopt a clear policy to maintain the privacy of the user's data and protect it [18]. Furthermore, article 4 stipulates that: "The payment provider must organize the relation with the user according to the clear contractual foundation which containing these obligations on the user: Using the payment service and applications in a security form accordance with the requirements and the procedures of its using, and taking all the procedures to maintain the secret Codes and/or passwords and any other security requirements"[19].

In brief, these instructions stress on the security in the relation between the users and the payment service providers. The security must be a clause in the contract, and the contractual parties must adopt all the security procedures during the payment process in e-transactions.

On the other hand, the Instructions No. 1/2020 regarding of the provision of service provider companies for electronic wallet service stipulate in article 2: "These instructions aim to regulate the works of electronic wallet service in the security and transparency way"[20].In addition, article 4 obligates the service provider in protecting and encryption the user's payment orders [21]. As a rule, the payment process attracts more hackers to obtain the user's data which are used to complete the payment process. Therefore, these instructions are important to oblige the payment service provider in maintaining theuser's security when he pays the price of goods and services in e-transactions.

Moreover, the precedential decree No. 15/2017 regarding of e-transactions also obligates the institutions which conducts the electronic business transferring in taking all the measures which introducing the security services to the customers and maintaining the banking privacy[22].This decree confirms on the user's security during the payment process in e-transaction due to online payment is an essential prosses in carrying out the obligations of the parties. In addition, this process is the main period that concerns the users regarding of their security.

Furthermore, the Instructions No. 1/2018 regarding of licensing the payment service companies clarifies the security in many articles especially in article 17 that stipulates: "The payment service provider must provide a protection system, and securing the electronic operations against the cyber-attacks, and which enabling of saving and storing thesystem's data and participants in a secure form that guarantee its privacy and protection from the lost or stolen [23]." These instructions are important to abide the payment service provider in adopting adequatesecurity system that maintain the user's data against any cyber-attacks. As a rule, the payment service provider can obtain the license if he fulfils the requirements of these instruction especially the security of information. However, the payment service provider cannot obtain the license of payment services if the system security is an inadequate.

The bank must examine and ensure the security of their system and website and maintain the integrity and reliability of their web servers. The banks must adopt new technologies, while also having the sufficient staffs that are able to handle these systems [24].

In general, the operation of online payments attracts the attackers due to their greed in collecting a high sum of money during online payment. Therefore, there are many types of threats facing the operation of online payment in e-transactions, such as denial-of-service attack (DoS attack), Man-In-Midle attack, Phishing, Pharming, viruses and Trojan Horses.

A denial-of-service attack (DoS attack): This type of attacks makes a server overload and useless by asking it to repeat the tasks many times, using the most of resources, and finally the system cannot work properly. The attackers attempt to downtime the servers due to making the security feature unavailable [25]. Similarly, Man-In-Middle attack, the Attacker enters into the current connection and he can tap the connection, access, read and changing of data [26].

In addition, the attacker in phishing pretends to be a reliable organization, and attacks using emails or malicious websites to obtain personal information. However, the hacker in Pharming redirects the user of Internet connection to a counterfeit website. Hackers can Pharm by changing the host file on the computer of the victim. Hackers make use of both pharming and phishing to steal online information [27].

On the other hand, the virus can spread through email or by downloading infected files, which lead to data changes of hard disk failure. Worms are independent programs that are activated without a need for a host program, and it spreads from computer-to-computer independently by exploiting security vulnerabilities or the errors of

formation in the operating systems [28].

Hackers design the Trojan horses as a beneficial application for the users in their computer. It is designed to spy on sensitive data such as passwords, which will enable the hackers to access the information remotely, whereas drive-by downloads are malware infections that occur when the user visits specific websites. In fact, the contents of the websites are legal, but there are malicious codes embedded into it [29].

Based on the preceding discussion, it is argued that there are many types of security threats to individuals using the Internet for transactions, and most of these threats are viable when they are paying for goods online. Therefore, it is the responsibility of the payment institution to ensure that their system is protected against all forms of attacks from the outside.

In fact,the issue of security threats is pertinent in Palestine. It was reported that the percentage of individuals aged 18 years and above in the Palestinian territory who are threatened by hacking and illegal access into their data was 2.6% in 2019. In addition, the percentage of individual who are exposed to spy on their data was 1.7%. On the other hand, 2% of individuals had their personal information stolen such as passport number and password, while 1.1% had their internet communication Intercepted [30].

These statistics indicate that the individuals in Palestine face many types of security threats in e-transactions, especially threats from illegal access and stolen personal. More protection is needed in Palestine if it is to be a viable option.

A password is an important layer of protection for users during e-transaction, and the important issue is avoiding insecure password. Therefore, the users require to adopt more difficult password that forbidden the attackers from tracking it [31].In addition, using One Time Password is important to protect the users in e-transactions due to the password is used one time and the user cannot use the same password across the site, as they chose a random password every login [32].

furthermore, using a One-Time Password represents the most common protection against attacks. This Password is used once and is valid for five minutes. First, the user enters the user ID and Pin number for authentication, and then they are sent their one-time password via SMS to their cell phones [33].

The security of e-transaction is an important issue for the consumers, merchants, and institutions. Security breaches means breaking the illegal access to private information by unauthorised person, such as names, addresses, passwords, and credit cards [34].Online banks and online payment institutions should adopt the adequate system hardware, operating, and application software, and the networks and communication systems that can protect the user and the payment institution against any attacks. The payment institution should have an agreement with an independent security company that can ensure the security of network device, web server, and the web application [35].

Identificationand authentication, encryption, and firewalls mechanism are important methods to ensure the security of e-banking. The identification of online banks is a form of known Internet address or Uniform Resource Locator (URL), whereas the identification of users depends on their login ID and password to ensure that only one person has access to one account. E-banks also adopt the Secure Socket Layer (SSL) browser, which encrypts the messages between the user and online banks to prevent anyone else from accessing the information exchanged between the banks and the users. Basically, a multi-layered security architecture, which includes firewalls, filtering routers, encryption and digital certification protects the information of users from any illegal access [36].The security of online payment depends on the cooperation between both banks and users, especially when the users are aware of how to protect themselves during payment [37].

Users should not store or reveal their personal information, such as PIN numbers or passwords, to anyone. In addition, it is important that passwords are changed regularly, and ensure that a user has logged out of his account once he is done with his transactions [38].

Online banking and financial institution need to pay more attention to the issues of security during of e-transaction. In fact, the money attracts more hackers who focus on breaching financial institutions. The security against threats during an electronic transaction, especially online payment, is essential. Banks and payment providers should take all precautions during online payment to protect themselves against the security threats, and to protect the users as well, because the high level of security protects all parties and increases the confidence of users in payment institutions.

In fact, the Palestinian laws give more attention regarding the issues of online banking, especially security in the websites. The Presidential Decree No. 9/2010 regarding of Banking Law allows the electronic services of banking without mentioning any issues of electronic banking security, such as the security of the online system against any threats; which may face the clients

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 432-443 www.ijaem.net ISSN: 2395-5252

when accessing the website of the bank to transfer money to pay for the goods in e-transactions. On the other hand, the regulations of the Palestinian Monetary Authority No. 5/2009 regarding of security and safety, clarifies the obligations of the banks in security and safety in general, without discussing the security of the website of the banks in online banking services.

The instructions of the Palestinian Monetary Authority No. 5/2009 regarding of the security and safety requirements, stipulates: "The banks are obliged to preserve the computer system, reports, tapes and CDs by: keeping the main server of the bank in a safe place, and insuring its continuous function. In addition, to put and implement the instructions and procedures of control which prevent unauthorised persons from accessing it to protect the data and information from any change" [39].

These instructions obligate the bank to adopt all the procedures of safety of the server system to prevent any access to this system by unauthorised persons. However, these regulations are unclear about the security of the bank's computer system offering online banking services. Therefore, adding further regulations that obligate the bank in providing a higher level of security in their websites against any threats is an important issue; in particular there are many banks in Palestine offering online banking services such as the Arab Bank.

It is noteworthy to see that the Arabic Agreement of Fighting Information Technology Crimes provides for the types of cybercrimes; they include illegal access to information technology. The penalty becomes severe if this access causes any deletion, change, copy or transfer of data. In addition, producing, selling or purchasing any tools or programs to commit crimes of information technology is a type of these crimes [40].

This agreement clarifies the types of crime in information technology. As a rule, producing the programs that aim to access or destroy data is illegal, such as producing viruses to destroy the data at the website of online banking. This agreement helps protecting the data of the users against unauthorised access in case of e-transactions; when they use the website of the bank to pay the price of goods and services. In addition, fighting information technology crimes needs international cooperation as internet is an open international space. In general, the laws that punish the cybercrimes are not enough to protect the website of online banking against any threats that may face the users during the payment the price of goods in e-transactions. Therefore, the bank is obliged also to take all necessary procedures to protect the website against any threats when it offers online banking services.

IV. ENCRYPTION AND ELECTRONIC SIGNATURE

The Palestinian precedential decree No.15/2017 regarding of the electronic transactions defines the electronic signature as: "A collection of electronic data whether it was letter, numbers, symbols or any other similar form associated with the electronic transaction in the form that allows to identify the signatory who signed it, and distinguish him from others in a purpose of approval on the content of electronic transaction" [41].

On the other hand, Article 2/a of UNCITRAL Model Law on Electronic Signatures stipulates: "Electronic signature", meaning data in electronic form in, affixed to, or logically associated with, a data message, which may be used to identify the signatory in relation to the data message, and to indicate the signatory's approval of the information contained in the data message [42].The electronic signature, in other words, is the data in the form of letters, numbers, symbols, and signals that are included in data messages, and are used to identify the identity of signatory and his acceptance of the information and data in the data message.

It is argued from all of these definitions that electronic signature is attached to electronic data or data message by the signatory. The electronic signature identifies the fact that the signatory accepts all the information inside the message.

Moreover, the certification authority plays a critical role in the creation of the certification for electronic signature. The role of these authorities is to verify that the signatory owns the electronic signature by issuing a certificate. The Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001) identifies the role of Certification authority in verification of electronic signature [43]"As a type of solution to some of these problems is the use of one or more. One type of solution to some of these problems is the use of one or more third parties to associate an identified signatory or the signatory's name with a specific public key. That third party is generally referred to as a "certification authority", "certification service provider" or "supplier of certification services" in most technical standards and guidelines (In a number of countries, such certification authorities are being organized hierarchically into what is often referred to as a "public-key infrastructure"

(PKI))"[44].

On the other hand, the precedential decree No. 15/2017 regarding of e-transactions stipulates that: The ministry [45] verifies that the electronic signature or the electronic record was fulfilment from a particular person, to follow the changes and errors in the electronic signature or the electronic record after it created [46]. This article clarifies the role of ministry in verifying the information of electronic signature and the information of the electronic record. Basically, the electronic signature and the electronic record should be valid to protect anyone who deals with the signatory and depend on his signature in e-transactions.

In addition, the ministry must close any company provides the electronic authentication services or electronic signature without obtaining the license. Furthermore, the ministry can cancel the license or stop it with limited time if the licensee violates the terms of license or the law [47]. The license is important to obligate the authentication service company in compel the terms of law, and to allow the ministry to control the works of these companies as they play an essential role in e-transaction as a third parties.

Moreover, the Instructions No. 1/2020 regarding of the provision of service provider companies for electronic wallet service obliges the service provider in protecting and encryption the user's payment orders [48]. The encryption of information is important to protect it during the payment process because there are many threats regarding the security of payment processes and hackers trying to intercept the payment data in e-transactions.

In fact, the payment service providers are obliged to ensure all information pertaining to electronic signature prior to implementing the payment process, especially in electronic transactions. The bank is obliged to verify the relations between an electronic signature and the person possessing the certificate. Moreover, the bank is expected to check the information from their respective sources vis-à-vis the clients from the Certification Authority Service Provider. In short, the bank would be liable if it implements the process of payment in e-transactions using forged signatures or wrong information, especially if it failed to verify all of the information that they got.

Generally, security is crucial in e-transactions, especially in the electronic payment. Electronic signature is important in electronic payment, as it maintains the security of the payer when paying in an e-transaction. In addition, electronic signature is important, as it reduces the disputes between the parties in a payment operation by verifying the identity of the parties while preventing any changes to the message.

The Palestinian precedential decree No. 15/2017 regarding of e-transactions clarifies the provisions of electronic signature and the role of the Certification Authority Service Providers. These provisions protect the consumer against fraud on the internet, in particular when the merchant provides the consumer with wrong information about his signature, or if he provides him with an expired signature certificate. The consumer can verify the certification from Certification Authority before signing the electronic contract and paying the price. Furthermore, the electronic signature introduces more protection to the consumer in e-transactions, as no one can read the content of information, or make any change in the content of the message. This issue is important in the period of the payment of goods in e-transactions; as the consumer sends the information of payment in a cryptographic way, and no one can read this information without collecting the keys.

V. PRIVACY ANDCONFIDENTIALITY

The consumers rely on his experience in computer and new technology in his adoption of electronic banking. A consumer faces many concerns during the usage of electronic banking, such as the integrity of the password, privacy, data encryption, hacking, and the protection of personal data. Therefore, the consumer needs experience in computer and Internet connection in the course of electronic banking [49].

The financial institutions should maintain the privacy of the users during the electronic transferring. The Palestinian precedential decree No. 15/2017 regarding of e-transactions stipulates: Any financial institution practices the electronic transferring of money, obliged in: Adopting all the procedures to introduce the security services to the customers and maintain the banking privacy [50]. Furthermore, the Instructions No. 3/2020 regarding of organizing the relation of payment service companies with the users stipulate that the service provider must adopt a clear policy to maintain the privacy of the user's information and protect it [51].

In addition, the Instructions No. 1/2018 regarding of licensing the payment service companies oblige the payment provider and all his workers in protecting the privacy of the customer's information and documents. In addition, they are not allowed from disclose the information or allow others from seeing it. However, disclosure the information requires a written permitting from the

customer or a decision of court. Furthermore, there are some exceptions on the requirement of protecting the privacy such as disclosure the information to the Monetary Authority [52].

These articles are important to protect the privacy of the users during the payment in e-transactions. In addition, these articles oblige the payment service provider in adopting all the security procedures and protecting the privacy of the users. It can be concluded from these articles, that the payment service provider would be liable in case of disclosure the user's information without any permission from the law or the users.

The precedential decree No. 15/2017 regarding of e-transactions clarifies the liability of the financial institution in the case of a breached account caused by a lost credit or debit card. The liability in this case depends on the wrongdoing or negligence of the institution that leads to the access of the account of the clients. However, the financial institution is not liable in the case of illegal usage of the client's account due to their negligence.

Article 30/1 of the precedential decree No. 15/2017 regarding of e-transactions stipulates that: "The client is not liable for any legal restriction [53] on his account through an electronic transfer that happened after he informed the financial institution about the possibility of accessing his account by an intruder, or losing his card, or the probability of knowing his pin number, and demanding from the financial institution to stop the service of electronic transfer [54]."

In addition, article 30/2 of the precedential decree No. 15/2017 regarding of e-transactions stipulates: "The bank is not liable for illegal use of the client's account if it is proved that the client contributed in this use and the institution fulfilled its obligations to avoid any illegal use for this account [55]."

Moreover, article 29/2 of the precedential decree No. 15/2017 regarding of e-transactions also obliges the institutions which conducts the electronic money transfaring inadopting the measures to introducing the security services to the customers and maintaining the banking privacy [56]. Therefore, the financial institution would be liable under the provisions of contractual liability in case of breaching the privacy of customers. These institutions should protect the privacy and the information of its customers during the process of electronic transactions. In fact, the customer provides the institution with their personal information prior to and after the signing of the contract. It is therefore the responsibility of the institution to maintain the privacy of the customers.

furthermore, the Presidential Decree No. 9/2010 regarding of Banking Law obliges the bank in protecting the privacy of its customers regarding their personal and financial information. Article 32 provides: "All current and previous board of directors members of the bank, key officials, staff, auditors, consultants, in banks and lending agencies have to protect the confidentiality of their client's information which reaches them by the nature/virtue ?of their jobs, and it is not allowed for any of them to reveal this information or to allow anyone outside the bank or lending agency to see such information, this confidentiality is valid to anyone who by the nature of his /her job directly or indirectly can view such information, except if it is according to the following: a. A written approval from the client b. A judgment by a Palestinian court [57]."

Usually, the customer provides the bank with his personal information when he aims to open an account at the bank. Therefore, this article is important to protect the privacy of the customer in case of online banking, especially personal information, the details of their account number and the number of the payment card. In addition, this law forbids all the staff in the bank who knows any information about the client from disclosing this information; and the members of staff are also forbidden from enabling anyone from viewing this information.

It is worth noting that, the Presidential Decree No. 9/2010 regarding of Banking Law provides some instances that enable the banks of disclosing the information of the client as an exception of protecting privacy, and these instances are limited by law. Therefore, the banks are obliged to protect the privacy of their clients except if there is any legal reason according to the Presidential Decree No. 9/2010 regarding of Banking Law. This decree provides: "The following cases are exceptions in paragraph (2) of this article with the commitment to confidentiality of information: a. Disclosure for legal duties to an external auditor according to this law. b. Disclosure of information and documentation requested by the Palestinian Monetary Authority or its assigned staff. c. Issuing a certificate or revealing a reason for refusal to cash any cheques upon the request of the client d. Limited disclosure of information in accordance to the money laundering law and its instructions [58]."

Regarding this article, the banks cannot disclose the information of their clients, except if there is any legal reason; and they can just disclose this information for the specific persons and reasons. Therefore, the banks would be liable if

they disclose the information of their clients as they breach their privacy, except if they prove that disclosure is under a legal reason and for the authorised person or entity, such as the Palestinian Monetary Authority.

It can be argued that Presidential Decree No. 9/2010 regarding of Banking Law and the Instructions No. 1/2018 regarding of licensing the payment service companies stipulate the similar provisions about protecting the privacy of the users by the payment service providers. These articles are important in protecting the privacy of the users when they pay the price of goods and services through the Internet.

Generally, banks secure their clients' personal information when they open an account. Moreover, clients are not willing to disclose their information, and the banks are obliged to maintain the privacy of their clients. Therefore, this law protects the privacy of the consumers against any disclosure of the client's information to unauthorised parties in e-transactions, especially in financial transactions.

VI. CONCLUSION

The electronic bank bears the liability for breach of contract for any harm caused to the client upon using the site of the electronic bank. The liability is contractual if the conditions exist and are the correct contract between the client and the bank, and that the bank has breached his obligations towards the client. One example is its failure to transfer the amount of money to the merchant from the account of the client within a limited time or its failure to transfer this money. In this case, the bank would be liable, and it is obliged to pay compensation for this harm, which happened to the client, according to the liability for breach of contract.

The liability of electronic bank might be tort if the bank, caused harm to the other without any contract between the bank and harmed person. An example is when the contract between them is void or terminated.

Protecting the privacy of users is crucial in the development of e-transaction, which motivates the individual to purchase goods and services through Internet. The laws protect the privacy of the users in re-transactions, in particular during the payment of the price of goods. Therefore, the banks are obliged to protect the user's information against any threats. The Palestinian Presidential Decree No. 9/2010 on Banking Law obligates the banks to protect the privacy of users when they provide the bank with their information. This law provides the protective provisions in the banking law as obligations of the banks in all works, without clarifying the special protection in e-transactional issues. Furthermore, the precedential decree No. 15/2017 regarding of e-transactions regulates the provisions ofprivacy protection during the electronic money transferring as the environment of the internet needs special provisions besides the general ones.

The payment institutions are obliged to protect users when they are paying online, which will increase user satisfaction and also shield themselves from liabilities. Digital signature is crucial in electronic payments as it helps maintain security in the course of online payments, as it verifies the identity of the parties, and keeps any payment messages from being altered.

Most of the Palestinian banks offer online banking services, and every user who has an account can access the website of the bank and manage his financial operations electronically anywhere. In fact, the Palestinian laws regulate this issue with independent provisions, especially the liability of payment service provider relating to the security and privacyprotection in e-transaction. The researcher discussed many instructions from the Palestinian Monetary Authority which regulates the user's security and privacy in e-transactions with independent provisions as a special issue.

The Palestinian laws and instructions regarding of the banks detailed the issues of outsourcing the bank's services to the third-party service provider and oblige the payment service providers in protecting the privacy and the security of the users during of outsourcing.

In fact, the issue of security and privacy has a substantial effect on the development of e-banking and payment service providers in Palestine. Therefore, the cooperation between the government, legislators, banks and the individuals is necessary to overcome such problems and to develop e-banking in Palestine and e-commerce in general.

As a result, the issues of security and privacy require the legislations which regulate the legal matters of payment service providers in Palestine such as the security of the websites against any risks including viruses and hackers. Moreover, the banks are obliged to protect the privacy of the users when they open an account and provide the bank with their personal information. On the other hand, the users need information and some experience in using internet banking and maintain their security during payment and money transfers between many accounts. Likewise, the users need information about protecting their information when accessing the website of the bank

including protecting their passwords and usernames and the secret number of their credit cards, besides of protecting their computers against any viruses.

REFERENCES

[1]. Palestinian Central Bureau of Statistics. (January 2020). Household Survey on Information and Communications Technology, 2019. Main Findings Report. http://www. pcbs.gov.ps/ PCBS_2012/Publications_AR.aspx?CatId=21&scatId=287. accessed on 29/1/2021

[2]. The Instructions No. 1/2018 regarding of licensing the payment service companies. The Palestinian Monetary Authority. 30/7/2018. Article: 1

[3]. The Instructions No. 3/2020 regarding of organizing the relation of payment service companies with the users. The Palestinian Monetary Authority. 27/7/2020. Article: 1

[4]. OECD "Report on Consumer Protection in Online and Mobile Payments. OECD Digital Economy Papers, no. 204, (2012): 10. OECD Publishing. http://dx.doi.org/10.1787/5k9490gwp7f3-en(accessed 29 Jan 2021).

[5]. Charles Chong, Hui-Na Chua and Cheng-Suan lee, "Towards Flexible mobile Payment Via Mediator based Service Mobile," slideShare, http://www.slideshare.net/sarper/towards-flexible-mobile-payment-via-mediatorbased-service-model.(accessed 29 Jan 2021).

[6]. The Instructions No. 1/2018 regarding of licensing the payment service companies. Article: 14/1

[7]. The Instructions No. 1/2018 regarding of licensing the payment service companies. Article:14/2

[8]. See Presidential Decree No. 9/2010 regarding of Banking Law. Article 19/1

[9]. See the Instructions No. 5/2010 regarding of Automated Connectivity and Outsourcing. The Palestinian Monetary Authority. 11/5/2010. Article 4/3/5.

[10]. The Presidential Decree No. 9/2010 regarding of Banking Law. This Decree was published in the Palestinian Official Gazette No. 0 on 27/11/2010, 5. Article: 1

[11]. The Instructions No. 1/2018 regarding of licensing the payment service companies. The Palestinian Monetary Authority. 30/7/2018. Article: 1

[12]. Capgemini and the Collaborative Business Experience. (2012). Global Trends in the Payment Card Industry: Issuers. At: 5. https:// www.capgemini.com/ wpcontent/uploads/ 2017/07/Global Trends in the Payment Card Industry Issuers.pdf. (accessedon:31/1/2021).

[13]. Yi-Jen Yang, "The Security of Electronic Banking," 4, http:// csrc.nist.gov/ nissc/1997/ proceedings/ 041.pdf (accessed on: 29 Jan, 2021

[14]. Symantec. Internet Security Threat Report Internet Report. Vol. 24. Feb. 2019. At: 14. https://docs.broadcom.com/doc/istr-24-2019-en.(accessed on: 1/2/2021).

[15]. Dickinson Turinawe and Rogers Mwesigwa, "Information on internet banking, Security and Privacy, Quality of internet connection, Perceived value and Internet Banking Acceptance in Uganda," International Journal of Economics and Management Sciences, vol. 2, no. 11 (2013): 32. Management Journals,>http://www.managementjournals.org/ijems/211/IJEMSi2n11i3i131813.pdf<

[16]. Sonny Zulhuda, "E-Payment Gateway Service in Malaysia and the Analysis of its Legal Framework," Australian Journal of Basic and Applied Sciences, v. 6, no. 11 (2012): 235, >http://ajbasweb.com/old/ajbas/2012/Special%20oct/233-238.pdf<.

[17]. The Instructions No. 3/2020 regarding of the relation between payment services companies with the users. The Palestinian Monetary Authority. 27/7/2020. Article:2

[18]. See the Instructions No. 3/2020 regarding of the relation between payment services companies with the users. The Palestinian Monetary Authority. 27/7/2020. Article:3

[19]. The Instructions No. 3/2020 regarding of the relation between payment services companies with the users. The Palestinian Monetary Authority. 27/7/2020. Article:4

[20]. The Instructions No. 1/2020 regarding of the provision of service provider companies for electronic wallet service. The Palestinian Monetary Authority. 21/4/2021. Article: 2

[21]. See the Instructions No. 1/2020 regarding of the provision of service provider companies for electronic wallet service. The Palestinian Monetary Authority. 21/4/2021.Article: 4

[22]. See the precedential decree No. 15/2017 regarding of e-transactions. This decree was published in the Palestinian Official Gazette No. 14, excellent number, on 9/7/2017, 2.

[23]. The Instructions No. 1/2018 regarding of licensing the payment service companies. Article: 17
[24]. Seminar, "Impact of e-Banking and e-Commerce on Central Banking Funtions," Hotel Istana, Kuala Lumpur, (9 January 2001). Bank Negara Malaysia, http:// www.bnm.gov.my/? ch=en_speech&pg= en_speech_all& ac=34&lang=en (accessed 19 Feb 2021).
[25]. M.Sc. Aleksandar Lukic. Benefits and Security Threats in Electronic Banking. International Journal of Managerial Studies and Research (IJMSR) Volume 3, Issue 6, June 2015, PP 44-47. >https://www.arcjournals.org/pdfs/ijmsr/v3-i6/7.pdf <
[26]. A. Mallik, A. Ahsan, M. M. Z. Shahadat & J. C. Tsou. Understanding Man-in-the-middle-attack through Survey of Literature. Indonesian Journal of Computing, Engineering and Design. Vol. 1. Issue 1, April 2019.Pp. 44-56. >https://pdfs.semanticscholar.org/761f/6b676a08e69ae1ffe5ade4b15900b413940d.pdf?_ga=2.108962567.486869857.1612431598-1734951013.1612431598 <.
[27]. Amtul Fatima, "E-Banking Security Issues – Is There a Solution in Biometrics?" Journal of Internet Banking and Commerce, vol.16, no. 2 (2011): 4. Array development,> http://www.arraydev.com/ commerce/ JIBC/2011-08/Fatima.pdf <.
[28]. Vrîncianu1, M., Popa, L. A, "Considerations Regarding the Security and Protection of E-Banking Services Consumers' Interests," Amfiteatru Economic Journal, vol. 12, no. 28 (2010): 391. Amfiteatru Economic, >http://www.amfiteatrueconomic.ro/temp/Article_971.pdf<.
[29]. Ibid.
[30]. Palestinian Central Bureau of Statistics. (2020). Household Survey on Information and Communications Technology, 2019 Main Findings Report. http:// www.pcbs.gov.ps/ PCBS_2012/ Publications_AR. aspx?CatId=21&scatId=287.(accessed on: 29/1/2021.
[31]. Verena Distler, Gabriele Lenzini, Carine Lallemand, and Vincent Koenig. (2020). The Framework of Security-Enhancing Friction: How UX Can Help Users Behave More Securely," New security paradigms workshop, NSPW '20, October 26–29, 2020, Online, USA. https:// www.nspw.org/ papers/2020/nspw 2020-distler.pdf. (accessed 14 February 2021).
[32]. Abe Singer and Matt Bishop. (2020). Trust-Based Security; Or, Trust Considered Harmful," New security paradigms workshop, NSPW '20, October 26–29, 2020, Online, USA. https://www.nspw.org/papers/2020/nspw2020-singer.pdf (accessed 14 February 2021).
[33]. Safa Hamdare, Varsha Nagpurkar, Jayashri Mittal, "Securing SMS Based One Time Password Technique from Man in the Middle Attack," International Journal of Engineering Trends and Technology (IJETT), vol. 11, Issue, 3 (2014). >http://www.ijettjournal.org/volume-11/number-3/IJETT-V11P230.pdf<. 155
[34]. Rashad Yazdanifard, Foong Kar Hoe, Mohammad Rabiul Islam and Seyed Pouya Emami, "Customer's Information Security Management System in E-commerce," International Conference on Software and Computer Applications IPCSIT, IACSIT Press, Singapore, vol. 9 (2011): 188, http://www.ipcsit.com/vol9/35-B30009.pdf (accessed 12 February , 2021).
[35]. Rajpreet Kaur Jassal and Ravinder Kumar Sehgal, "Online Banking Security Flaws: A Study," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, Issue, 8 (2013): 1019,>http://www.ijarcsse.com/docs/papers/Volume_3/8_August2013/V3I2-0257.pdf<.
[36]. Vrîncianu and Popa, 395.
[37]. Jassal, Sehgal, 1021.
[38]. Ruby Shukla and Pankaj Shukla, "E-Banking: Problems and Prospects," International Journal of Management & Business Studies (IJMBS) vol. 1, Issue. 1 (2011): 25, >http://www.ijcst.com/ijmbs/research1/ruby.pdf<.
[39]. The Instructions No. 5/2009 regarding of the Security and Safety. Palestinian Monetary Authority. 1/4/2009. http://www.pma.ps/Portals/1/Users/002/02/2/Legislation/Instructions/Banks/2009/instructions-5-2009.pdf
[40]. See Arabic Agreement of Fighting the Information Technology Crimes. Articles 6-9. This agreement is signed on: 21/12/2010. Palestine ratified this agreement on: 21/5/2013.
[41]. The precedential decree No. 15/2017 regarding of e-transactions. Article: 1. This article is in parimateria with article 1 of the

precedential decree No. 17/2012 relating to national payment settlement law. This law was published in the Palestinian Official Gazette No. 8, excellent number, on: 9/12/2012

[42]. UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001. Article 2/a (Model Law on Electronic Signatures adopted by the United Nations Commission on International Trade Law).

[43]. UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001.

[44]. UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001. 26.

[45]. The ministry of the communications and information technology.

[46]. The Palestinian precedential decree No. 15/2017 regarding of e-transactions. Article: 8

[47]. The Palestinian precedential decree No. 15/2017 regarding of e-transactions. Article: 44

[48]. The Instructions No. 1/2020 regarding of the provision of service provider companies for electronic wallet. Article: 4

[49]. Sirajbeg Salimbeg Mirza, "A study on Customer Perception Towards E-Banking: Identifying Major Contributing Factors," Golden Research Thoughts, vol. 2, Issue. 5 (2012):2. <http://aygrt.isrj.net/Uploaded Data/1729.pdf<

[50]. The Palestinian precedential decree No. 15/2017 regarding of e-transactions. Article: 29

[51]. The Instructions No. 3/2020 regarding of organizing the relation of payment service companies with the users. Article: 3/1

[52]. See the Instructions No. 1/2018 regarding of licensing the payment service companies.

[53]. This article includes an error, and the text must be: The client is not liable for any illegal restriction on his account.

[54]. The Palestinian precedential decree No. 15/2017 regarding of e-transactions. Article: 30/1.

[55]. The Palestinian precedential decree No. 15/2017 regarding of e-transactions. Article: 30/2

[56]. The Palestinian precedential decree No. 15/2017 regarding of e-transactions. Article: 29/2

[57]. The Presidential Decree No. 9/2010 regarding of Banking Law. Article 32/2.

[58]. The Presidential Decree No. 9/2010 regarding of Banking Law. Article 32/3.

International Journal of Advances in Engineering and Management
ISSN: 2395-5252

IJAEM

Volume: 03 Issue: 03 DOI: 10.35629/5252

www.ijaem.net
Email id: ijaem.paper@gmail.com