Security Concerns in E-payment and the Law in Jordan

Mohammad Atwah Al-ma'aitah
Mis Department
Al-balqa Applied University
Amman - Jordan

***Abstract*—Recently communications and information technology became widely used in various aspects of life. The internet becomes the main network for information support. Using of internet enabled public and private organizations to develop its business and expand its activities. Private organizations applied the principles of e-commerce to improve the quality of services which provided to customers. While public sector organizations started to apply the principles of e-government in an effort to increase efficiency and effectiveness and achieve maximum equality among citizens. One of the major challenges raised by widespread use of e-government and e-commerce application is security issues especially e-payment. This paper discusses the present law in Kingdom of Jordan which deal with the problem of frauds and violation of consumers' rights and privacy when they making e-payment. In addition this paper tries to make comprehensive study on e-payments and the law to decide if there more legislation is needed.**

***Keywords*—E-payment systems; Cyber crime; Web security; Law.**

I. Introduction

E-payment systems (EPS) have become a most important factor in the growth of electronic commerce and e-government application. In addition EPS system may determine success and fail of these applications. An electronic payment system is an essential part in new business-to-consumer and business-to-business e-commerce [1] [2] [3]. The development of e-business contributed considerably to the development of electronic payment systems so as to meet the needs of e-procurement processes and to facilitate the completion of the transactions [4]. Tsiakis and Sthephanides argued that "the security and trust issues that are essential for every electronic payment mechanism in order to be accepted and established as a common medium of financial transactions" [5]. As a result of this development in this area, the diseased soul's owners were increased to ambitions to commit cyber crime and penetrate privacy of others especially that the numbers of workers in the field of information were increasing. Then more legislation is required to deal with these crimes.

II. Literature Review

A. Evolution of Electronic Payment

Organizations were used to deal with financial dealings in the traditional way such as paper work. But with beginning of communication and internet technology most of financial procedures dealt with it electronically. On the other hand the appearance of internet and the raise of electronic communications technology impact considerably the growth of E-payment [6].

B. Electronic payment systems (EPS)

The desired e-payment service appears after e-commerce shaped [7]. E-Payment is defined as "the transfer of an electronic value of payment from a payer to a payee through an e-payment mechanism" [8]. Prior researcher such as [7] [9] [10] categorize the instruments used for e-payment as shown in Fig (1).

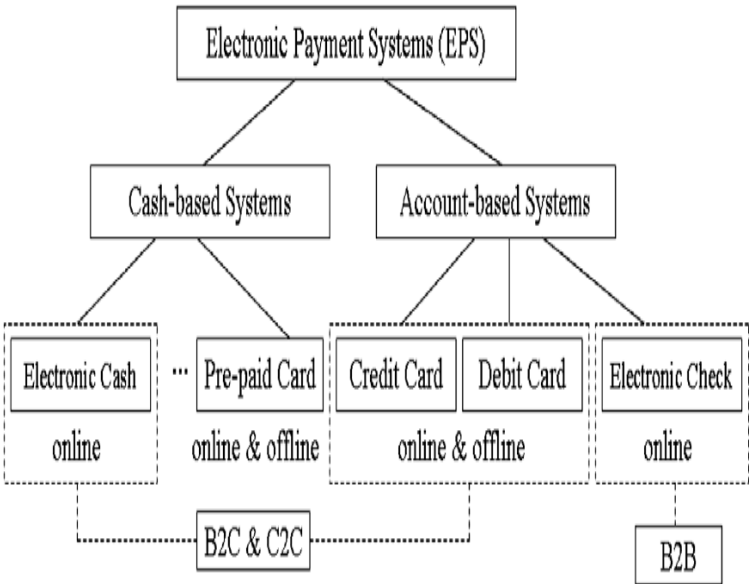

Fig.1. Classification of electronic payment systems: [7] [9] [10].

In addition [7] argued that " Electronic-cash, pre-paid cards, credit cards, and debit cards are widely used in B2C and C2C EC". According [11] he defined e-money as "Broadly, e-money is defined subject to exceptions as monetary value represented by a claim on the issuer that is (i) electronically stored; (ii) issued on receipt of funds for the purpose of making payment transactions; and (iii) accepted as payment by someone other than the issuer". New mechanisms discussed by [12] in deeply which called Web ATMs. Via this new technology the payment of transaction can obtain and send right in several seconds. It is a really suitable way of online payment tool enabling clients to assign or transfer funds, effect payments, and make account inquiries 24 hours a day, all year

Identify applicable sponsor/s here. If no sponsors, delete this text box (*sponsors*).

round. In addition they argued that "With Web ATMs and Web 2.0, we now have an opportunity to make amends. Modern electronic financial services will be more flexible and modular, allowing capabilities to be added as and when required on Web. Such safe payment services will not only extend their sales opportunities but also benefit to the whole economic benefits, cost-effective of banking industry. Most importantly, this does mean that there is a big breakthrough on the innovative payment instrument of money flow of e-commence".

Some Suggested steps by [13] that have to be taken by organizations to protect personal information in the particular security risks within organizations. In determining appropriate security measures, organizations should:

- Identify the security risks to the personal information that is being held.
- Build up policies and procedures to reduce those identified risks.
- Apply suitable IT security settings governing system access; and
- - Monitor and measure performance against relevant Australian and International standards

Ma'aitah and shtat [14] agreed that Importance of Authorization and Importance of encryption influence the perceived security of E-finance transactions; these features can contribute toward enhancing the perceptions of the users that the web and online transactions including E-Finance transaction are secure, and encourage them to use the online system and do financial transactions online.

Tsiakis and Sthephanide [5] discussed the concept of security and trust in electronic payments. Although they discussed some of requirement and properties necessary to build successful electronic payment systems as listed follow:

1) Integrity: confidence that information has not been changed after the data was signed.

2) Authentication: The process by which one person verifies that another entity is who they claim to be.

3) Fraud prevention and tolerance: prevention of parties from fraud and from economic losses in the case the system crashes or the network fails.

4) Privacy: information must not be revealed to not permit people.

5) Divisibility: option of numerous denominations.

6) Transferability: spending of token without the need to contact the issuer.

7) Payment anonymity: the payee will know only pseudonym of the payer

C. Web Security

Web security means the capability of the web to maintain and protect the individual sensitive information from any changing, waste, disclosure, destruction or in use by unauthorized persons such as Internet intruders andhackers. The web security system must avoid unauthorized users to use the computer system and manage access to the network from inside and outside the organization [15], [16].

Security is the life of E-Commerce and it has grown to be the most significant concern for its expansion [17]. However the two most vital areas preventing the successful implementation of E-Commerce worldwide are the Internet methodologies and E-Commerce dealings security

III. E-PAYMENT AND SECURITY THREATS

The lack of security measures still plays as a major risk factor in electronic payment process. Hence; the privacy of personal data on the level of the individual or institutions is not attained. This will lead to loss of individual data or spy on financial and administrative processes. Nevertheless, barriers could arise in term of buying and selling through electronic means such as the abuse of the privacy of individuals and the lack of electronic laws structure that are available in many countries to detect them from such a great danger as piracy and spy ware.

In a result of that people started to be afraid of electronic payment even though it is equipped with a lot of advantages been offered. This was confirmed by a study that was conducted by the researcher

A survey questioner was distributed with a random sample of 300 respondent in which different levels of instruction was applied to the questions to focus on the reason behind the lack of use of electronic payment (buying and selling) to answer whether a lack of security, privacy and laws are necessary to protect the operations of electronic payment. The following results show that there is a significant relationship between the lack of security, privacy and laws are necessary to protect the operations of electronic payment see Table below I:

TABLE I. Response answer

1. 62%	answered	yes
2. 29%	answered	no
3. 9%	answered	do not know

All findings obtained refer that respondent's fear of using the electronic payment concept because of the security and privacy of data, nevertheless; the increasing number of hacker's and data penetration possibility which transferred through the Internet.

Nowadays; technological innovation has played a major role in the development of business. One major innovative tool is the Websites. Websites is a great technological innovation that changed the way we do business [18]. Because of The increase use of Websites, millions of virtual stores are already available and the number is increasing dramatically. Unfortunately, parallel numbers of cyber crimes done by hackers are also accruing. Website security is still an open issue since we lack comprehensive international laws against cyber criminals. If laws do exist against hackers, the implementation is quite hard considering the complexity of the cyber world

Hackers refer to any computer fanatic who breaks into computer systems for the sake of gaining information or

conducting playful mischief and stealing or corrupting data [19]. In relation to the previous definition hackers are everyone feels that the security forces are not yet able to provide reasonable protection for internet users. Hence, the aim of this research focuses on the legal role in the protection of data privacy and security through electronic payment.

IV. Law regarding Security of e-payments in Jordan

In the case of Jordan, like many developing countries, a lack of legal legislation for the protection of any form of electronic payment. At the same time taken in consideration cyber crime, increase with the information technology revolution and the use of networks for data transmission between individuals and institutions that form a real threat to all users. Therefore a special law has to be issued to protect the privacy of citizens and institutions and protection of their moral and financial.

A. Cyber crime can be divided into two main types as follows:

- Crime committed through the use of electronic media as a tool to commit the crime as it is threatened by electronic means or slander and libel and others.

- The crime that targeted electronic means or their contents as the destruction of an information system or steal information from a site or network or electronic information system or infringing on privacy and confidentiality.

B. Jordan Information Systems and Cyber Crime Law:

On 16/9/2010 issued by the Government of Jordan Information Systems Crimes Act No. 30 of 2010 meaningful issuing this law limit the crimes that occur through the use of the Internet, which use spread due to the large and rapid development in the field of Communications and Information Technology.

The Information Systems Crimes Act on maintaining the rights and privacy of personal and financial rights as well as all that would affect the security and stability of the country by selecting the sanctions to curb violations and / or the excesses of the Internet users.

Noting here that the enactment of such a law it is absolutely imperative that the Jordanian Penal Code, as amended text in Article III that "no offense, but the text does not spend any penalty or measure did not provide for the law to them while committing the crime, and is considered the crime completely if has actions implemented without of time to get the result, "meaning no crime or punishment except the text so it has assigned men of law the validity of acts considered crimes inventory and determine the punishment through the specific provisions into law

C. Crimes addressed by Jordan Information Systems and Cyber Crime Law:

Law deals mainly some electronic crimes that have evolved and became her legal terms set it apart from traditional crimes legislation does not criminalize traditional, and of those crimes:

1) *Penetrate the e-mail site.*
2) *Piracy.*
3) *Denial of Service.*
4) *Illegal access to information system or network computers.*
5) *Send viruses.*
6) *Sabotage devices and systems remotely, or using electronic systems.*
7) *Destruction of information that is available to the public affecting national security.*
8) *Steal information stored by electronic means.*
9) *Impersonate capacity.*
10) *Change the information stored or transmitted by electronic means.*

The law has been divided into 17 articles were allocated legal articles 5, 6, 7 electronic crimes and states:

1) *Article 5:*

Any person who intentionally captures or intercept or eavesdrop on what is sent through the Internet or any information system shall be punished by imprisonment for not less than one month nor more than one year or a fine of not less than (200) two hundred dinars and not more than (1000) thousand dinars, or both penalties.

2) *Article 6:*

A. All of intentionally got without a permit through the Internet or any information system, data or information related to credit card data or information to be used in the implementation of financial transactions or electronic banking is punishable by imprisonment for a term not less than three months and not exceeding two years or a fine not less than (500) five hundred dinars and not more than (2000) thousand dinars, or both penalties.

B. All of the used through the Internet or any information system intentionally without a legitimate reason data or information regarding the credit card or the data or information to be used in the implementation of financial transactions or electronic banking for himself or to other data, information or money or services belonging to others punished imprisonment for a term not less than one year and a fine of not less than (1000) thousand dinars and not more than (5000) five thousand dinars.?

3) *Article 7:*

Doubled the punishment for the crimes stipulated in Articles (3) to (6) of this law, the right of every person who committed any of them while doing his job or his work or exploitation of any of them.

V. The Official Security Agencies that Deal with Cyber Crime

There is in the General Security Directorate Jordanian administration called CID and U where a special section offenses electronic named Department computer crimes and their website is (http://www.cdd.psd.gov.jo), and through correspondence, official and field visits to this section got excellent results I did not expect that we in Jordan are dealing security with this volume of electronic crimes were as shown in table(II):

TABLE II. The number of cases from 1999 to 2013.

No.	Year	Cases No.	Samples No.	Detected ratio
1.	1999	5	13	71.4%
2.	2000	28	452	63.6%
3.	2001	29	179	77.7%
4.	2002	36	7756	73.5%
5.	2003	43	145	71.4%
6.	2004	56	125	63.6%
7.	2005	66	723	71.4%
8.	2006	74	813	62.9%
9.	2007	84	85	65.6%
10.	2008	96	975	83.3%
11.	2009	105	753	71.4%
12.	2010	111	604	75%
13.	2011	113	347	78.5%
14.	2012	167	262	60%
15.	2013 To date	84	160	56.3%
Total		1097	13392	-

Through the above table which we have collected from the Department of Electronic Crimes and found that it received from several quarters, namely, (CID, preventive security, counter-narcotics, protection of the family, the tourist police, legal affairs, crime scenes, the courts, the General Intelligence Department and Customs).

It was one of the most important issues that deal with the following section:

The issue of ATM card theft by devices have been added to an ATM machine and revealed through the crime scene downtown Amman.

The issue of counterfeiting of currency: and this case had been received from the Drug Enforcement Administration include computers and flash memory belonging to suspects in counterfeiting, forgery and using a program (Encase) confirms that the suspected counterfeiting banknotes.

The issue of electronic articles and comments insulting: Use Program (Email Tracker Pro) your track websites and in cooperation with the Telecommunications Regulatory Authority (TRA) is determined by a person who worked on the publication of an article or comment the abuse of others.

Fraud case in the Forex market Stock Exchange firms: where he worked as a suspect in this case to design Web pages and fake sites similar speculation the company's global Forex and using a program (Encase) devices suspects were examined by a court order.

Email issues and sexual exploitation of adults and children: have been discovered using the program (Email Tracker Pro) and the FTK program.

Indecent assault as a result of issues dating through social networking sites: was discovered using a program (Encase)

The issue of recognition of registration of murder: were discovered using a program (CSL) which used to matching voice to samples.

VI. Discussion And Conclusion

The results of this research demonstrate that there are a number of reasons for not using information and communication Technologies (ICT) such as electronic payment; despite of it is convenience, and saving time and efforts of users. First, one of the most important reasons this study confirms, is that the use of such technologies threats the security and privacy of information of users. Earlier to 2001, Jordan did not have any law to protect deal-mail. However, on December 11, 2001, the Jordanian legislator enacted the provisional law of Electronic Transactions No. 85. This was the first law within the package of legislation of information technology in Jordan, and the second Arabic law after Tunisia that concerns with electronic commerce. While this progress is considered important in this domain, it has been remained in the form of a temporary law.

Second, the issuance of this law was not enough to convince citizens to accept the use of electronic payment. That is, the practice of Jordanian customers was only limited to the use of ATM at banks and Visa cards to complete their purchases in different shops. In contrast, people in a number of developed countries such as US, UK, and Franc use electronic payment and do not use cash to compete their transactions. This indeed refers to the presence of contemporary laws that aim to maintain the security and integrity of the information and the privacy of individuals in all information and communication technologies (ICT) such as electronic payment.

Third, the law in its current content and application still unable to address all forms of threat that users of information and communication technologies face. This is due to the absence of clear and comprehensive texts that express all expected forms of electronic crimes, in addition to the lack of judges specialized in electronic crimes and lawyers in this area.

Fourth, some banks and companies in Jordan and particularly in the private sector point out that recently piracy became very common. For instance, there are some hackers who get into customers' accounts through the confidential numbers of their credit cards and transfer money from their accounts to other accounts.

This led Jordanian banks to maintain the reputation action settlement directly with customers whose accounts penetrated by hackers. Most banks which its accounts under threaten

suggest their customers, by sending them short messages to their Mobiles, to not give any figures or confidential information about their accounts to any party whatsoever.

Finally, security and privacy are considered two critical elements in dealing with electronic transactions in general and each other up. The lack of appropriate security means that privacy will be the victim and this leads to the unwillingness of citizens to accept the idea of dealing with the electronic commerce in general, and electronic payment in specific. Although the Jordanian law of 2010 addresses some of the threats related to the security and privacy of information through electronic transactions, it is still insufficient. That is, courts face difficulties to give its judgment on relevant issues within appropriate time framework, as some cases take years to get a definitive legal judgment that saves monetary and non-monetary rights of the victims.

With the above discussion in mind, this research based on monitoring the progress of some issues in the courts, recommends the following:

1) Prepare judges to be specialists in both fields: law and computer. This can be happened by adopting the Ministry of Justice to the idea of sending them to obtain their higher education in law with the main focus on studying contemporary issues related to the use of computer, networks, internet, information security, and databases. The total course hours should be designed in a way that enables these students to be familiar with the nature and different forms of cyber crime exist in the real life. This helps them to deal with different cyber crime issues in the courts.

2) Amend the current laws to cope with the development of using information and communication technologies (ICT) in all areas. This leads to enhance the confidence of institutions and individuals to use electronic payment, that became crucial in distinguishing between developed and developing countries.

3) Protect the rights of individuals and organizations by exerting all the important and required efforts and providing legal security. This also leads to increase the number of people using (ICT) such as electronic payment.

4) Used IP version 6 and web2.0 technology.

5) Enhance culture about computer crimes during public and private sectors

REFRENCES

[1] Katsaros, P. "A roadmap to electronic payment transaction guarantees and a Colored Petri Net model checking approach", Information and Software Technology, Vol. 51, (2009), pp: 235–257.

[2] Kousaridas, A., Parissis, G., and Apostolopoulos, T. "An open financial services Architecture based on the use of intelligent mobile devices", Electronic Commerce Research and Applications, Vol.7, (2008), pp: 232–246.

[3] Cotteleer, M. J., Cotteleer, C. A., and Prochnow, A. "Cutting checks: challenges and choices in B2B e-payments", Communications of the ACM, Vol.50, Issue 6, 2007, pp: 56–61.

[4] Simon, N., and Sutter, G. "Electronic Payments — the Smart Card", Computer Law & Security Report Vol. 18, No.4, pp: 2002.

[5] Tsiakis, T., and Sthephanides, G. "The concept of security and trust in electronic payments", Computers & Security, Vol.24, pp: 10-15.

[6] Shamim, F. "The ICT environment, financial sector and economic growth: a cross-country analysis", Journal of Economic Studies, Vol. 34, No. 4, 2007, pp. 352-370.

[7] Kim., C., Tao., Wang , and Shin, N. "An empirical study of customers' perceptions of security and trust in e-payment systems", Electronic Commerce Research and Applications, Vol. 9, (2010), pp: 84–95.

[8] Weir, C. S., Anderson, J. N., and Jack, M. A. "On the role of metaphor and language in design of third party payments in E-Banking: usability and quality", International Journal of Human-Computer Studies, Vol.64, No.8, (2006), pp: 70–784.

[9] Guan, S., and Hua, F. "A multi-agent architecture for electronic payment", International Journal of Information Technology and Decision Making, Vol.2, No.3, (2003), pp: 497–522.

[10] Dai, X., and Grundy, J. "Net Pay: an off-line, decentralized micro-payment system for thin-client applications", Electronic Commerce Research and Applications, Vol.6, (2007),Pp: 91–101.

[11] Kemp., R. "Mobile payments: Current and emerging regulatory and Contracting issues", computer law & security review Vol.2, No.9, (2013), pp: 175:179.

[12] Tsai., W, Huang. B, Tsaur. T, and Lin., S. "The application of Web ATMs in e-payment industry: A case study", Expert Systems with Applications, Vol.37, (2010), pp: 587–597.

[13] Kennedy., G. "Asia-Pacific news", computer law & security review, Vol.27, (2011), pp: 563:570.

[14] AL-ma'aitah, M. and Shatat, A. "Empirical Study in the Security of Electronic Payment Systems ", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No (2011).

[15] Hopwood, W. "Security in a Web-Based Environment, Managerial Finance", Vol.26, (2001), pp.42-52.

[16] Efraim, T. Michael, C.H. and Jae, L.K. "Electronic Commerce: A Managerial Perspective", Prentice Hall, 4th Ed, 2006.

[17] Jun., S. and Punit, A. "The more secure the better? A study of information security readiness", Industrial Management & Data Systems, Vol.111 Issue: 4, (2011), pp.570-588.

[18] Wells, J. Valacich, J. and Hess, T. "What signal are you sending? how website quality influences perceptions of product quality and purchase intentions", Journal MIS Quarterly, Vol.35, (2011), pp:373:396.

[19] Mookerjee, V., Mookerjee, R., and Bensoussan, A. "When Hackers Talk: Managing Information Security Under Variable Attack Rates and Knowledge Dissemination", Journal of Information Systems Research, Vol.22, Issue 3, (2011),pp: 606-623 .