sustainability

MDPI

Article

E-Commerce Liability and Security Breaches in Mobile Payment for e-Business Sustainability

Se-Hak Chun

Department of Business Administration, Seoul National University of Science and Technology, 232 Gongreung-Ro, Nowon-Gu, Seoul 01811, Korea; shchun@seoultech.ac.kr; Tel.: +82-2-970-6487

Received: 9 January 2019; Accepted: 25 January 2019; Published: 29 January 2019

Abstract: This study investigates liability issues in electronic transactions when security or privacy breaches occur. As data is transferred using various devices, such as PCs, mobile phones, tablets, sensors, smart meters, and cars, and various architecture, such as the cloud, IoT, as well as in well-defined network structures in electronic commerce, privacy and security breaches happen. These have become a major hindrance to the development and use of commercial activities on the Internet. There have been many security breach cases, such as those of Target Corporation's security and payment system (2013), eBay's cyberattack (2014), Uber's hacking incident (2016), Facebook's personal data use and privacy breach (2018), and many others. Therefore, when a dispute regarding electronic transactions arises between a customer and a firm, the allocation of liability is very important for the sustainability of e-businesses. Many cases show that firms are held liable for those incidents. However, the liability allocation rule tends to vary slightly from country to country depending on the application areas. EU countries seem to favor customers. In the United States, there are actually no uniform federal laws relating to business cybersecurity. Also, in the case of cryptocurrency, liability tends to lie with customers. Why is the ruling different? In this regard, this paper analyses the legal framework for security and privacy breaches for sustainable e-businesses. In particular, this paper focuses on the optimal liability in terms of enhancing social welfare when considering both sides—the customer and the firm (or service provider). This paper shows that liability can be generally imposed on the firm's side when the possibility of security or privacy breaches is high, and the customer's loss is relatively large. However, the liability depends on the customer's attitude towards risk, customer's losses, and the efficiency of security investment.

Keywords: E-commerce transactions; Fraud transactions; Liability; Payment systems; Security breaches

1. Introduction

The Internet has led to the e-commerce revolution, which is the result of the development of a network with increasing connectivity and functionality [1]. Forrester Research [2] predicts that U.S. online retail sales will increase to more than $500 billion by 2020 compared with $373 billion in 2016, and online sales will account for 17% of all US retail sales by 2022, up from a projected 12.7% in 2017. Also, mobile commerce sales account for 6% of total global retail sales and nearly 60% of e-commerce, following a rise of 40% in 2017 [3]. International Data Corporation [4] expects smartphone shipment volumes to grow 4.2% in 2017 and 4.4% in 2018, and will increase with a compound annual growth rate (CAGR) of 3.8% over the period 2016–2021. Also, in recent years, social media websites have enabled Internet users to communicate and interact with their friends, meet new acquaintances, share user-generated content, such as photos, videos and text, and be increasingly well informed about news and trends [5]. A Pew Research Center survey [6] shows that about two-thirds of American adults (68%) are now social media users, and they at least occasionally get news on social media; this is about the same share as at this time in 2017.

However, as the size of e-business and social media increases, security and privacy remain critical obstacles that hinder more accelerated growth of e-business. Mikalef et al. [7] elucidate how specific aspects of social media websites foster user intention to browse products. They found that the convenience of social media, the selection of products, trend discovery, and the feeling of adventure are significant factors which are positively related to browsing products through social media. Other aspects, such as information availability, customized advertisements, and socializing, are not significant factors. However, they did not consider security and privacy factors with regard to browsing content on social media websites. In reality, data breaches happen daily, and are all too common. However, it is difficult to determine how much risk or damage such breaches cause for companies, insurers, and users or account holders. According to Cybercrime Report [8], cybersecurity ventures predict cybercrime's global cost will reach $6 trillion by 2021. Yahoo's breaches knocked an estimated $350 million off Yahoo's sale price [9]. Data breaches frequently occur in companies such as eBay, TJX Companies, Inc., Uber, JP Morgan Chase, Sony's PlayStation Network, Home Depot, Adobe, and many others [9]. Also, according to cybersecurity company Carbon Black [10], $1.1 billion worth of cryptocurrency was stolen in the first half of 2018. Target's example of a massive data breach in the USA shows how personal information should be secured if the business is to maintain its integrity and reputation, because customers are less likely to shop at Target if they feel that their credit card/debit card security has been compromised. Also, recent failures on the part of Facebook in ensuring privacy for user data shows how privacy and security assurance is important for electronic transactions. In addition, online fraud is becoming another major hindrance to the development and use of commercial activities on the Internet [11]. The incidence of fraud is reported as being 20 times higher in online trades than in offline trades [11].

In particular, the explosive growth of smart mobile devices has changed business approaches due to the convenience of performing transactions, such as electronic banking, mobile payments, and transmitting confidential business data [12]. For example, mobile banking and payments have increased, with a growth projected at 50% per year [13]. The main benefit of mobile payments is that it is convenient and more portable than even the smallest netbook. Even though mobile payments are considered to be unsafe, customers believe that the convenience outweighs the associated security risk. However, some customers have been reluctant to use these devices because of the inconvenience of downloading applications, the small screen, and the possibility of loss or theft, while others remain skittish about mobile banking because they do not believe that mobile payments are safe and secure [14]. As observed in e-commerce, a lack of customer trust in the financial and legal infrastructure associated with online payments poses a major issue, and unfortunately, many security vulnerabilities are now seen as a threat to users of mobile banking [1]. Although many customers in the United States use mobile banking, many of them do not believe mobile payments using a smartphone are secure [15]. Therefore, it may be necessary to insure against damage caused by hacking or fraud when it comes to mobile transactions. In this regard, sophisticated technological barriers can be broken at the weakest link in the network security chain, i.e., the people engaged in the transaction [16]. Thus, the components of human trust and security technology should be regarded as important aspects of the cost involved in establishing trust in mobile transactions [16]. Kim et al. [17] suggested three high-level categorizations of e-commerce security: security managerial issues, fundamental security issues, and security technology issues. These three issues should be equally stressed; a lack of caution in one could cause irreversible security incidents. In general, most literature on security in electronic commerce or mobile networks has focused on technical issues rather than managerial or legal issues. Changes in technology and mobile transactions require changes in jurisdiction, regulations, and other standards associated with requirements for new or enhanced payment services [18]. Although system security can be addressed by installing firewalls and intrusion detection systems, monitoring security alerts and promptly implementing security patches, human factors, and liability issues also remain a major challenge to information security [1]. Thus, this paper investigates a liability rule for e-business transactions when security or privacy breaches occur in online transactions, considering

both sides—the customer and the firm—and discusses how the liability rule can be applied to mobile payments and fraudulent e-commerce transactions.

The remainder of this paper is organized as follows: Section 2 presents security issues in terms of e-business and mobile payments, and Section 3 analyzes the optimal liability rule followed by a discussion of some of the implications of the liability rule with cases in Section 4. Finally, in Section 5, conclusions are offered and future research is discussed.

2. Security Issues with Regard to Mobile Payment and E-Business

2.1. Security Threats with Regard to Mobile Payment

Recently, mobile networks have aimed at high-speed, ultra-low latency, and high capacity capability, and are capable of transmitting large amounts of data in a shorter time compared to existing wireless networks. In particular, 5G networks are expected to emerge as new types of technologies become available for services, such as Connected Cars, Internet of Things (IoT), and Virtual and Augmented Reality (VR/AR). However, in spite of the excellent technical advantages of 5G networks, recent research has pointed out problems in applying 5G technology. In particular, various experts have pointed out 5G security-related issues. Horn introduces security issues in 5G network components and argues that security should be considered when designing secure 5G networks [19]. Munisankaraiah describes the security weaknesses in the physical layer that make up a 5G network [20]. The issue of security needs to be dealt with as a matter of urgency, as there is a great deal of interest and massive investment in 5G.

In mobile network transactions, customers can access the web-enabled services of a merchant and order products or services and make payment using a high-speed network [21]. This information can be transmitted from the mobile device to a base wireless station and the application gateway of the merchant through mobile networks [22]. As mobile networks have become open and have evolved from the simple communication of placing and receiving voice calls to users interacting using multimedia data, the risk of security attacks has increased. However, customers and merchants should expect transaction information and transaction data to be confidentially and securely delivered [23].

Users of mobile devices increasingly face various types of threat, such as botnets, spyware, malicious applications, phishing, and social networking [12]. Mobile devices can be classified into two types according to their potential usage and possible security issues: one is heavyweight devices, which are not always operated within an organization's intranet. The second is lightweight devices, which are categorized by having high mobility, including wireless phones and PDAs. In addition, there are two categories of security challenges in terms of content security, which refers to the protection of data stored in the device, and channel security, which refers to preventing unauthorized users gaining access to the content. Both are a function of the type of wireless technology used in these devices [21]. Mobile devices have specific features, such as mobility, personalization, connectivity, and technology convergence, which make them more vulnerable to security attacks [18].

2.2. Mobile Payment

Internet technology has the potential to fundamentally change banks and the banking industry and can lead to lower banking costs [23]. Mobile payment has become a new form of e-banking available to banks, performed preferably either through a Short Message Service system (SMS) or the mobile internet, or via the installation of specialized programs in mobile phones. Although both banks and customers benefit from the use of e-banking services, customers and companies must take security into account in order for e-banking to be a valuable alternative and not a potential disaster [23]. Precautions for safeguarding the security of transactions and the identification of customers are essential. Security may be considered the most critical factor that negatively influences prospective customers of e-banking services [23]. People hear about hackers, crackers, computer viruses, identity theft, phishing attacks, spyware, malware, and many other security issues regarding the Internet.

Nevertheless, it is not only the Internet that is fraught with security breaches: there are numerous incidents regarding fraud through the use of fake ATM cards or the theft of identity data through the infiltration of inadequately-guarded information systems.

Mobile banking and payment services are currently under transition, with a history of numerous unsuccessful solutions [24]. Because there is a trade-off between security and ease of use in the mobile environment, this issue needs to be investigated from both legal and behavioral perspectives [24]. Thus, governing rules are required, as well as correct identification of the subscriber, which may be done through mobile devices, sensors, and other devices.

3. The Optimal Liability Model

3.1. The Basic Model (No Investment Model)

The liability issue between the customer and firms is more important in the case of disputes raised by security breaches or fraud transactions in online transactions, because privacy concerns increase, as do security threats. When security or privacy breaches occur in online networks, the firm may have less incentive to secure the managing process if security liability lies with a customer, and the customer has less utility from buying products or services online. On the other hand, if security liability lies with the firm and is favorable to the customer, the firm may invest more in securing the process to retain its customers.

We focus on three major parties to online transactions: the firm (or data provider), the customer, and the regulatory regime. We assume that customers' willingness to pay is uniformly distributed along $[0, V]$, i.e., $v \in [0, V]$. Thus, V represents the maximum willingness to pay on the part of customers and can be the potential market share of the product, because we assume customers are uniformly distributed [25,26].

There are two customer segments in the market. Customers in the first segment have disutility when they buy products or services online, because of their reluctance to expose their privacy, fear of security breaches, the risk of hacking and viruses, and fraudulent transactions, etc. We call this group the 'risk averse' segment, and assume that this first group has the proportion m in the market, and that they will invest to protect their privacy. Security or privacy breaches occur with the probability of ϕ, and customers face a risk cost, r. Then, the customers' net expected utility is

$$U_r(v) = \phi(v - p - r - a) + (1 - \phi)(v - p) = v - p - \phi r, \tag{1}$$

where p is the price at which customers buy.

Customers in the second type perceive no risk when they buy products online, and thus we call the second group the 'risk free' segment. Thus, this second group has the proportion 1-m in the market. The net expected utility of the second group depends only on the price, thus it is

$$U_{nr}(v) = v - p.$$

We assume that the firm produces a product or service with constant marginal cost. Without loss of generality we assume no fixed costs and normalize marginal cost to zero. Then, the firm will expect the following profits:

$$\begin{aligned} \Pi &= P(mq_r + (1 - m)q_{nr}) \\ &= P(m(V - p - \phi r) + (1 - m)(V - p)) \end{aligned} \tag{2}$$

where q_r represents the demand of the first group, and where q_{nr} is that of the second group.

Table 1 explains the parameters in the models we hereafter analyse.

Table 1. Summary of Notations in the Models.

Notation	Definition (Explanation)
x	The amount a customer invests in security
y	The amount a firm invests in security
ϕ	The probability of a security or privacy breach when a customer has liability and invests in any kind of security.
θ	The probability of a security or privacy breach when a firm has liability and invests in any kind of security.
r	The risk cost, damage or psychological loss from a security incident
p	The price of a service or item.
q	The demand for a service or item on the part of the customer
v	The customer's reservation price for a service or item: $v \in [0, V]$. V represents the maximum willingness to pay on the part of customers
m	The proportion of the 'risk averse' segment.
Π	The subscript 1, 2, 3 denote case 1, 2, 3 and subscript c, f represent when the liability lies with the customer and when liability lies with the firm. So, Π_{1c} and Π_{1f} are for case 1, Π_{2c} and Π_{2f} are for case 2, and Π_3 for case 3 when a government has responsibility for a sec urity breach; Π_{ic} and Π_{if} are for the investment model.
CS	CS denotes consumer surplus. So, CS_{1c} denotes consumer surplus of case 1 when the liability lies with the customer. CS_{1f} for case 1 when liability lies with the firm. CS_{2c} and CS_{2f} are for case 2. CS_3 for case 3. CS_{ic} and CS_{if} for the investment model.
SW	SW denotes social welfare. SW_{1c} and SW_{1f} are for case 1. SW_{2c} and SW_{2f} are for case 2. SW_3 for case 3 and SW_{ic} and SW_{if} are for the investment model.

3.2. Analysis of Case 1: $r < \frac{V-p}{\phi}$

3.2.1. When Liability Lies with the Customer

When liability lies with the customer, the customer's net expected utility in group 1 is

$$U_1 = v - p - \phi r. \tag{3}$$

Then, the firm sets the optimal price that maximizes its profit. The first-order condition is

$$\frac{\partial \Pi_{1c}}{\partial p_{1c}} = \frac{\partial (m p_{1c}(V - p - \phi r) + (1-m) p_{1c}(V - p_{1c}))}{\partial p_{1c}} = 0, \tag{4}$$

where subscript 1 denotes case 1, and subscript c represents when the liability lies with the customer. From the first-order condition, the optimal price and profits are derived as follows:

$$\begin{array}{c} p_{1c}^* = \frac{V - m\phi r}{2} \\ \Pi_{1c}^* = \frac{(V - m\phi r)^2}{4}. \end{array} \tag{5}$$

The regulatory regime then considers the social welfare that sums consumer surplus and a firm's profit. The consumer surplus of the first and second groups are as follows:

$$\begin{array}{rl} CS_{rc} & = m \int_{p_{1c}+\phi r}^{v} (v - p - \phi r) dv \\ & = \frac{m}{2}(V - p_{1c} - \phi r)^2 \\ & = \frac{(V - (2-m)\phi r)^2}{8} \\ CS_{nrc} & = (1-m) \int_{p_{1c}}^{V} (v - p) dv \\ & = \frac{(1-m)}{2}(V - p_{1c})^2 \\ & = \frac{(1-m)(V + m\phi r)^2}{8} \end{array} \tag{6}$$

where r denotes the 'risk averse' segment and nr is the 'risk-free' segment.

Using the optimal price, the total consumer surplus of case 1 is derived as follows:

$$CS_{1c} = \frac{\left(V^2 - 2Vm\phi r - \left(3m^2 - 4m\right)\phi^2 r^2\right)\right)}{8}. \tag{7}$$

Then, social welfare is derived as follows:

$$SW_{1c} = \Pi_{1c} + CS_{1c} = \frac{\left(3V^2 - 6m\phi rV + 4m\phi^2 r^2 - m^2\phi^2 r^2\right)}{8}. \tag{8}$$

3.2.2. When Liability Lies with the Firm

In this case, the 'risk averse' customer group is free from the security risk because the firm has liability for the security loss. Therefore, customers in group 1 have the same utility as those in group 2. Without loss of generality, the firm compensates the loss only for group 1 because customers in group 2 do not consider their security or privacy risk. The probabiliy of a security breach can be different according to who has the liability. In this regard, θ denotes the probability of a security breach when the firm has liability, and can be lower than ϕ when the customer has liability because of the efficiency of security investment [27]. Then, the profit of the firm is derived by

$$\begin{gathered} \Pi_{1f} = p_{1f}\left(mq_{rf} + (1-m)q_{nrf}\right) - mq_{rf}\theta r \\ = mp_{1f}\left(V - p_{1f}\right) + (1-m)p_{1f}\left(V - p_{1f}\right) - m\left(V - p_{1f}\right)\theta r \\ = \left(p_{1f} - m\theta r\right)\left(V - p_{1f}\right) \end{gathered} \tag{9}$$

where subscript 1 denotes case 1, θ denotes the probability of a security breach, and subscript f represents a case when the liability lies with the firm.

The firm sets the optimal price that maximizes its profit. The first-order condition is

$$\frac{\partial \Pi_{1f}}{\partial p_{1f}} = \frac{\partial\left(\left(p_{1f} - m\theta r\right)\left(V - p_{1f}\right)\right)}{\partial p_{1f}} = 0. \tag{10}$$

From the first-order condition, the optimal price is derived as follows:

$$p_{1f}^* = \frac{V + m\theta r}{2}. \tag{11}$$

The regulatory regime then considers the social welfare that sums consumer surplus and a firm's profit. Consumer surplus of the first and second group is as follows:

$$\begin{gathered} CS_{1f} = CS_{1rf} + CS_{1nrf} = m\int_{p_{1f}}^{v}(v - p_{1f})dv + (1-m)\int_{p_{1f}}^{V}\left(v - p_{1f}\right)dv \\ = \frac{m}{2}\left(V - p_{1f}\right)^2 + \frac{(1-m)}{2}\left(V - p_{1f}\right)^2. \end{gathered} \tag{12}$$

Using the optimal price, the total consumer surplus of case 1 is derived as follows:

$$CS_{1f} = \frac{(V - m\theta r)^2}{8} \tag{13}$$

Then, social welfare is derived as follows:

$$SW_{1f} = \Pi_{1f} + CS_{1f} = \frac{(V - m\theta r)^2}{4} + \frac{(V - m\theta r)^2}{8} = \frac{3(V - m\theta r)^2}{8}. \tag{14}$$

3.2.3. Results and Discussion of Case 1

The regulatory regime then compares two cases and assigns liability so that that social welfare is maximized. Comparing the above two cases of social welfare, the following proposition is obtained:

Proposition 1.

(i) When $\theta = \phi$, liability lies with the customer.

(ii) When $\theta < \phi$, liability lies with the firm if $m > m^*$.

Proof. (i) $SW_{1c} - SW_{1f} = \frac{m(1-m)}{2}\phi^2 r^2 > 0$.

(ii) Let $\theta = \phi - \alpha, SW_{1c} - SW_{1f} = \frac{3V^2+\phi^2 r^2 m(4-m)-6Vm\phi r}{8} - \frac{3\left(mr(\phi-\alpha)-V^2\right)}{8}$. If $m > m^* = \frac{4r\phi^2-6V\alpha}{4\phi^2+3\alpha^2-6\alpha\phi}$, $SW_{1c} - SW_{1f} < 0$. □

Proposition 1-(i) states that if there are no differences in the probability of a security breach between when customers have liability and when firms have liability, the regulatory regime can impose the liability on the customer in the case of $< \frac{V-p}{\phi}$, because the firm can raise the price when the liability is on the firm's side, which leads to a reduction in consumer surplus and social welfare. So, when risk costs are low, the regulatory regime imposes the liability on the customer, anticipating more consumer surplus with a lower price.

Proposition 1-(ii) states that if the firm has more advantage in terms of security technology than the customer, and thus the probability of a security breach is lower, social welfare can be different depending on the proportion of the customer's distribution. If we regard θ as the function of a firm's security level when it has liability, generally θ can be assumed to be lower than ϕ, the security level when the customer has liability. Consequently, the liability can be shifted, depending on how many customers are concerned with regard to their privacy. Thus, if there are many customers who are concerned about security or privacy (when $m > m^*$), then the regulatory regime imposes the liability on the firm from a social welfare perspective.

3.3. Analysis of Case 2: $r > \frac{V-p}{\phi}$

3.3.1. When Liability Lies with the Customer

The first group does not buy products or service because its willingness to pay is negative. Thus, the profit function of the firm is as follows:

$$\Pi_{2c} = p_{2c}(1-m)(V-p_{2c}) \tag{15}$$

From the first-order condition, the optimal price is derived as follows:

$$p_{2c}^* = \frac{V}{2} \tag{16}$$

Then, the regulatory regime considers social welfare that sums consumer surplus and the firm's profit. The consumer surplus of the first and second groups is as follows:

$$CS_{2c} = (1-m)\int_{p_{2c}}^{V}(v-p_{2c})dv = \frac{(1-m)}{2}(V-p_{2c})^2 \tag{17}$$

Then, social welfare is derived as follows:

$$SW_{2c} = \Pi_{2c} + CS_{2c} = \frac{(1-m)V^2}{4} + \frac{(1-m)V^2}{8} = \frac{3(1-m)V^2}{8} \tag{18}$$

3.3.2. When Liability Lies with the Firm

The first group will buy the product or use the service because the firm compensates for the loss when a security breach occurs. Thus, the profit function of the firm in case 2 is the same as in case 1 when the liability lies with the firm and is given as follows:

$$\begin{gathered}\Pi_{2f} = p_{2f}\Big(mq_{2f} + (1-m)q_{2f}\Big) - mq_{2f}\phi r \\ = mp_{2f}\Big(V - p_{2f}\Big) + (1-m)p_{2f}\Big(V - p_{2f}\Big) - m\Big(V - p_{2f}\Big)\phi r \\ = \Big(V - p_{2f}\Big)\Big(p_{2f} - m\phi r\Big)\end{gathered} \tag{19}$$

From the first-order condition, the optimal price is derived as follows:

$$p_{2f}^{*} = \frac{V + m\phi r}{2} \tag{20}$$

Thus, social welfare is the same as in case 1 when the liability lies with the firm, and is given as follows:

$$SW_{2f} = \Pi_{2f} + CS_{2f} = \frac{3(V - m\phi r)^2}{8} \tag{21}$$

3.3.3. Results and Discussion of Case 2

In case 2, both consumer surplus and social welfare are the same as in case 1 when liability lies with the firm. Comparing the social welfare differences between the two cases, we obtained the following proposition:

Proposition 2.

(i) *If* $m > m^{**} = \frac{V}{\phi r}\Big(2 - \frac{V}{\phi r}\Big)$, *then* $SW_{2c} < SW_{2f}$

(ii) $\frac{\partial m^{**}}{\partial \phi} < 0$ *and* $\frac{\partial m^{**}}{\partial r} < 0$.

Proof. $SW_{2c} - SW_{2f} = -\frac{3m\left(V^2 - 2\phi rV + m\phi^2 r^2\right)}{8}$. □

In the case of $r > \frac{V-p}{\phi}$, the liability depends on how customer groups are distributed. Proposition 2-(i) states that if the size of the 'risk averse' group is relatively larger than m^{**}, the regulatory regime imposes the liability on the firm, while if the size of the "risk averse" group is smaller than m^{**}, the regulatory regime assigns the liability to the customer. This proposition implies that if more customers are concerned with their security and privacy risk, the regulatory regime assigns the liability to the firm, which compels the firm to invest more on security or privacy protection, aiming to obtain increased revenue from attracting the 'risk averse' customer group. Proposition 2-(ii) shows how the possibility of a security breach and the subsequent loss affects the liability assignment. It states that the liability could be increasingly imposed on the firm as the probability of a security breach and the amount of loss increases. This proposition explains a recent trend that governments have laid particular stress on a firm's responsibility for their security level as security incidents are reported more frequently, and customers are more concerned with their security or privacy risk.

3.4. Analysis of Case 3: When a Regulatory Regime Provides Products

We consider a case in which a government itself provides products or services. For many reasons, some governments still manage nationalized companies in industries such as banking, telecommunications, broadcasting, electric power, oil, railroads, or transportation. Thus, we investigate how social welfare can differ when a government itself manages firms, and is responsible for incidents including security or privacy breaches, fraud transactions, and whether it compensates for the loss.

Without loss of generality, we assume that the government will compensate only for the 'risk averse' group, because the risk-free group is not concerned with its privacy risk. We focus on comparing this case with case 1 when the liability lies with the customer. As shown in the previous section, liability can be imposed on the customer from the perspective of social welfare, as in case 1. Then, the profit function when a government owns a firm is as follows:

$$\begin{aligned} \Pi_3 &= mp_3(V - p_3) + (1 - m)p_3(V - p_3) - m(V - p_3)\phi r \\ &= (V - p_3)(p_3 - m\phi r) \end{aligned} \tag{22}$$

where subscript 3 denotes case 3 when a government has responsibility for a security breach.

The consumer surplus for case 3 is as follows:

$$CS_3 = \int_{p_3}^{V} (v - p)dv = \frac{1}{2}(V - p_3)^2 \tag{23}$$

Then, the government finds the optimal price to maximize social welfare function as follows:

$$SW_3 = (p_3 - m\phi r)(V - p_3) + \frac{1}{2}(V - p_3)^2 \tag{24}$$

From the first-order condition, the optimal price and social welfare are obtained as follows:

$$p_3^* = m\phi r \text{ and } SW_3^* = \frac{1}{2}(V - m\phi r)^2 \tag{25}$$

Comparing case 3 with case 1 when a customer has liability, we obtained the following proposition:

Proposition 3.

(i) *If* $m < m^{***} = \frac{1}{5\phi r}\left(V + 2\phi r - 2\sqrt{\phi^2 r^2 - (V - \phi r)V}\right)$, *then* $SW_3 > SW_{1c}$

(ii) $\frac{\partial m^{***}}{\partial \phi} > 0$ *and* $\frac{\partial m^{***}}{\partial r} > 0$

Proof. Omitted because of the simplicity of the calculation. □

Proposition 3-(i) states that a government can be responsible for a security breach when the size of the "risk averse" group is relatively small. Also, proposition 3-(ii) shows how the possibility of a security breach and the consequent loss affects the government's responsibility with regard to security loss. It states that as the probability of a security breach and the amount of loss increases, a government may be more involved in responsibility for the security breach. This result also implies that a government may regulate a private firm's prices, or impose liability on the firm, in order to enhance social welfare by giving them a subsidy, even in case 1. This proposition explains why some governments still manage their nationalized companies in industries such as banking, telecommunications, broadcasting, electric power, oil, railroads, or transportation. Thus, it implies that a government tends to nationalize firms and regulate prices when the possibility of a security breach and the consequent loss increases.

3.5. The Extended Model (Investment Model)

We consider a model in which customers and firms invest in security in order to lower the possibility of a security breach for the case when $r < \frac{V-p}{\phi}$.

3.5.1. When Liability Lies with the Customer

We consider a model in which a customer invests money in security (or makes precautionary efforts) to lower his or her damage from a security breach. Then, his or her net expected utility is

$$U_r(x) = \phi(x)(v - p - r) + (1 - \phi(x))(v - p) - x = v - p - \phi(x)r - x, \tag{26}$$

where ϕ is the security breach probability, r is the risk cost which customers face, p is the price, and x is the amount of monetized value when a customer makes precautionary efforts.

Without loss of generality, we assume customers in group 2 do not mind a loss of privacy and consequently do not invest in security. Let $\phi(x) = \frac{\beta}{1+kx}$. Then, a customer will invest the amount of $x^* = \frac{-1+\sqrt{k\beta r}}{k}$.

Also, the firm sets an optimal price that maximizes its profit. The first-order condition is as follows:

$$\frac{\partial \Pi_{ic}}{\partial p_{ic}} = \frac{\partial (m p_{ic}(V - p_{ic} - \phi(x)r - x) + (1 - m)p_{ic}(V - p_{ic}))}{\partial p_{ic}} = 0, \tag{27}$$

where the subscript i denotes the investment case, and the subscript c represents when the liability lies with the customer.

From the first-order condition, the optimal price and profits are derived as follows:

$$p_{ic}^* = \frac{V - m\phi r - mx^*}{2} \Pi_{ic}^* = \frac{(V - m\phi r - mx)^2}{4} \tag{28}$$

The regulatory regime then considers the social welfare that sums consumer surplus and the firm's profit. The consumer surplus of the first and second group are as follows:

$$\begin{array}{ll} CS_{irc} & = m \int_{p_{ic}^* + \phi r + mx^*}^{v} (v - p_{1c} - \phi r - mx^*) dv \\ & = \frac{m}{2}(V - p_{1c} - \phi r - mx^*)^2 \\ & = \frac{(V - (2-m)(\phi r + x^*))^2}{8} \\ CS_{inrc} & = (1 - m) \int_{p_{ic}^*}^{V} (v - p) dv \\ & = \frac{(1-m)}{2}\left(V - p_{ic}^*\right)^2 \\ & = \frac{(1-m)(V + m(\phi r + x^*))^2}{8} \end{array} \tag{29}$$

where r denotes the 'risk averse' segment and nr is the 'risk-free' segment.

Using the optimal price, the total consumer surplus of case 1 is derived as follows:

$$CS_{ic} = \frac{\left(V^2 - 2Vm\phi r - \left(3m^2 - 4m\right)\left(\phi^2 r^2 + x^{*2}\right) - x^*\left(2Vm - 8m\phi r + 6m^2\phi r\right)\right.}{8}. \tag{30}$$

Then, social welfare is derived as follows:

$$\begin{array}{c} SW_{ic} = \Pi_{ic} + CS_{ic} \\ = \frac{(3V^2 - 6m\phi rV + 4m\phi^2 r^2 - m^2\phi^2 r^2 - 4x^{*2}(4-m)m - x^*\left(6Vm - 8m\phi r + 2m^2\phi r\right)}{8}. \end{array} \tag{31}$$

3.5.2. When Liability Lies with the Firm

The firm invests the amount of money in security or privacy protection, aiming to obtain increased revenue from attracting customers. In the investment model, the profit function of the firm is similar to those in cases 1 and 2 when the firm has the liability and is as follows:

$$\Pi_{if} = \left(p_{if} - m\theta(y)r\right)\left(V - p_{if}\right) - y \tag{32}$$

where the subscript i denotes the investment model, the subscript f represents the case when the liability lies with the firm, and y is the amount of money the firm spends on security.

The firm sets the optimal price that maximizes its profit and the first-order condition is as follows:

$$\frac{\partial \Pi_{if}}{\partial p_{if}} = \frac{\partial\Big(\Big(p_{if} - m\theta(y)r\Big)\Big(V - p_{if}\Big) - y\Big)}{\partial p_{if}} = 0 \tag{33}$$

From the first-order condition, the optimal price is derived as follows:

$$p_{if}^{*} = \frac{V + m\theta r}{2}. \tag{34}$$

Also, the firm decides the amount of security investment, y.

$$y^{*} = \frac{-1 + \sqrt{k\beta rm(V - p_{if}^{*})}}{k} \tag{35}$$

To simply compare this case with the previous case when the customer has liability, we assume that the firm invests the same amount of money on security as the customers does. Thus, the maximum total amount of investment by the firm is as follows:

$$y^{**} = x^{*}mq_{if}^{*} = x^{*}m(V - p_{if}^{*}) > y^{*}. \tag{36}$$

We safely assume that if the firm invests the same amount of money on security, the probability of a security breach is lower than that which exists when customers have liability. Thus,

$$\theta(y^{**}) = \phi(x^{*}) - \alpha < \phi(x^{*}). \tag{37}$$

The regulatory regime then considers social welfare that is the sum of consumer surplus and a firm's profit. The consumer surplus of the first and second groups are the same as in the previous case, which is as follows:

$$CS_{if} = CS_{irf} + CS_{inrf} = \frac{(V - m\theta r)^{2}}{8}. \tag{38}$$

Social welfare is derived as follows:

$$SW_{if} = \Pi_{if} + CS_{if} = \frac{(V - m\theta r)^{2}}{4} - y^{*} + \frac{(V - m\theta r)^{2}}{8} = \frac{3(V - m\theta r)^{2}}{8} - y^{*}. \tag{39}$$

3.5.3. Results and Discussion

The regulatory regime compares two cases of social welfare and assigns the liability that maximizes social welfare. The following proposition is then obtained:

Proposition 4.

(i) If risk costs are low (high), the liability lies with the customer (firm).

(ii) As the efficiency of the security investment of the firm is high, the liability lies with the firm.

Proof. (i) Let $SW_{if}{}^{*} = \frac{3(V-m\theta r)^{2}}{8} - y^{**} < \frac{3(V-m\theta r)^{2}}{8} - y^{*} = SW_{if}$ and $y^{**} = x^{*}mq_{if}^{*} = x^{*}m(V - p_{if}^{*})$.

If $\theta = \phi$ (or $\alpha = 0$), $SW_{1c} - SW_{1f}{}^{*} = -\frac{m\left(m\left(x^{2}+6\phi rx+4\phi^{2}r^{2}\right)+2xV^{2}-4x^{2}-4\phi^{2}r^{2}-8\phi rx\right)}{8}$.

If $r > r^* = \frac{\sqrt{x}}{\phi}\left(\frac{\sqrt{V}}{\sqrt{2}} - \sqrt{x}\right)$, $SW_{ic} - SW_{if} < 0$ because $2xV^2 - 4x^2 - 4\phi^2 r^2 - 8\phi rx > 0$. Also, if $r \leq r^* = \frac{\sqrt{x}}{\phi}\left(\frac{\sqrt{V}}{\sqrt{2}} - \sqrt{x}\right)$, $SW_{ic} - SW_{if} \geq 0$. (ii) $\frac{\partial\left(SW_{ic} - SW_{if}{}^*\right)}{\partial\alpha} < 0$ because $\frac{\partial SW_{ic}}{\partial\alpha} = 0$ and $\frac{\partial SW_{if}{}^*}{\partial\alpha} > 0$. □

Proposition 4-(i) states that if the customers' risk costs are low, the liability lies with the customer, while if the customers' risk costs are high, the liability lies with the firm. From the perspective of social welfare, the regulatory regime imposes liability on the customer in order to enhance social welfare when customers face less privacy costs. This is in line with proposition 1-(i). Even in the case when the firm's investment efficiency is very low ($\theta = \phi$), the regulatory regime may impose liability on the firm to enhance social welfare if the customer's risk costs are large. These results are very similar to the previous propositions. Proposition 4-(ii) is in line with proposition 4-(i), which states that as the efficiency of the security investment of the firm becomes high, the liability lies with the firm. This implies that a regulatory regime may impose liability on the firm even in the case when risk costs are lower. This is because generally a firm has a great deal of knowledge with regard to security technology, and its investment efficiency is likely to be higher (α is high) than that of customers who make an effort in terms of security.

4. Implications of Analytical Results and Case Discussion

4.1. Summary of Analytical Results and Implications

Table 2 shows equilibrium prices, market share, profit, and social welfare. Generally, the equilibrium price (market share) when the firm has liability is higher (lower) than that when a customer has liability. The price in the investment model is higher (lower) when the firm (customer) has liability, while the market share in the investment model is lower (higher) when the firm (customer) has liability. Also, the profits and social welfare in case 1 and case 2 are the same when the liability lies with the firm. However, social welfare depends on the size of the risk averse group (m) and the risk cost (r).

Table 2. Equilibrium Results.

	Price, Profit, Social Welfare
Case 1	$p_{1c} = (V - m\phi r)/2, q_{1c} = (V - m\phi r)/2,$ $\Pi_{1c} = (V - m\phi r)^2/4, \mathrm{SW}_{1c} = \left(3V^2 - 6m\phi rV + 4m\phi^2 r^2 + m^2\phi^2 r^2\right)/8$
	$p_{1f} = (V + m\phi r)/2, q_{1f} = (V - m\phi r)/2,$ $\Pi_{1f} = (V - m\phi r)^2/4, \mathrm{SW}_{1f} = 3(V - m\phi r)^2/8$
Case 2	$p_{2c} = V/2, q_{2c} = (1 - m)V/2,$ $\Pi_{2c} = (1 - m)V^2/4, \mathrm{SW}_{2c} = 3(1 - m)V^2/8$
	$p_{2f} = (V + m\phi r)/2, q_{2f} = (V - m\phi r)/2$ $\Pi_{2f} = (V - m\phi r)^2/4, \mathrm{SW}_{2f} = 3(V - m\phi r)^2/8$
Case 3	$p_3 = m\phi r, q_3 = V - m\phi r,$ $\Pi_3 = 0, \mathrm{SW}_3 = (V - m\phi r)^2/2$
Investment Model	$p_{ic}^* = \frac{V - m\phi r - mx^*}{2}, \Pi_{ic}^* = \frac{(V - m\phi r - mx^*)^2}{4},$ $SW_{ic} = \frac{(3V^2 - 6m\phi rV + 4m\phi^2 r^2 - m^2\phi^2 r^2 - 4x^{*2}(4-m)m - x^*(6Vm - 8m\phi r + 2m^2\phi r)}{8}.$
	$p_{if}^* = \frac{V + m\theta r}{2}, \Pi_{if} = \frac{(V - m\theta r)^2}{4} - y^*, SW_{if} = \frac{3(V - m\theta r)^2}{8} - y^*$

Note: c denotes when liability lies with the consumer, while f denotes when liability lies with the firm.

To assign liability, the regulatory regime compares the social welfare of each model in Table 2. Table 3 shows how the liability can be shifted, depending on different situations. In the case 1 ($r < \frac{V-p}{\phi}$), if there are no differences in the investment efficiency between a customer and the firm ($\theta = \phi$), it is better to impose liability on the customer. However, if the firm's investment efficiency is high ($\theta < \phi$), then the regulatory regime can impose liability on the firm when the size of the 'risk averse' group is large ($m > m^*$). Case 2 ($r > \frac{V-p}{\phi}$) also shows similar results to case 1 when $\theta < \phi$, when the regulatory

regime imposes liability on the firm when more customers are concerned with their security and privacy risk ($m > m^{**}$). It does this in order to induce the firm to invest more on security or privacy protection. Also, case 3 implies that a government may subsidize the firm and impose liability on the firm when the size of the 'risk averse' group is relatively small ($m < m^{***}$), even when $r < \frac{V-p}{\phi}$ and $\theta = \phi$. Lastly, in the investment model, the liability lies with the customer (firm) if the customer's risk costs are high (low).

Table 3. Analytical Results of Models

	Models	**Results**
No Investment Model	Case *1c*: $r < \frac{V-p}{\phi}$ and $\theta = \phi$	Liability lies with the customer (when $\theta = \phi$)
	Case *1f*: $r < \frac{V-p}{\phi}$ and $\theta < \phi$	Liability lies with the customer (when $m < m^{*}$) Liability lies with the firm (when $m > m^{*}$)
	Case 2: $r > \frac{V-p}{\phi}$	Liability lies with the customer (when $m < m^{**}$) Liability lies with the firm (when $m > m^{**}$)
	Case 3: $r < \frac{V-p}{\phi}$ and $\theta = \phi$ government intervention	The government has liability (when $m < m^{***}$) The customer has liability (when $m > m^{***}$)
Investment Model	$r < \frac{V-p}{\phi}$	Liability lies with the customer (when $r < r^{*}$) Liability lies with the firm (when $r > r^{*}$)

Note: m^{*} denotes a threshold value for case 1, m^{**} for case 2 and m^{***} for case 3.

4.2. Case Discussion

The results of the analytical models are based on the social welfare perspective. Court judgments for actual disputed cases can differ from the results of the analytical models and show different liability assignments between a customer and a firm, depending on data breach situations and the country in which the security incident occurs. Generally, whether or not the existence of gross negligence is with the customer seems to be a key factor when it comes to allocating liability. We explore actual disputed cases from three perspectives in the form of the security breach level, a country's culture, and the application area.

First, from the technical perspective, customers tend to be responsible for a security breach in terms of access control related to the log-in process, because the court can assume that a customer's precaution costs are small. However, for security breach levels, such as software vulnerabilities, firm's poorly managed environments, and third-party integration, a firm could be liable because customers do not have sufficient knowledge to prevent security incidents [28].

Second, the liability allocation rule tends to vary slightly from country to country. For example, Europe's new privacy law, known as the EU's General Data Protection Regulation (GDPR), is in favor of customers, and aims to protect all EU citizens from privacy and data breaches. Its impact can be far broader, and battles with major IT companies, such as Facebook, Google, Yahoo, LinkedIn, MySpace, and others, are anticipated [29]. In the United States, there are no uniform federal laws with regard to security breaches. For example, the decisions of some courts in the Eastern District of Louisiana and the Northern District of Illinois show that customers are liable when their personal information has been compromised. In Green v. eBay Inc., the U.S. District Court for the Eastern District of Louisiana dismissed a putative class action brought on behalf of eBay customers whose data had been stolen when eBay user information was hacked. Similarly, in Strautins v. Trustwave Holdings, Inc., the U.S. District Court for the Northern District of Illinois dismissed the plaintiffs' class action lawsuit seeking damages due to a data breach that exposed in excess of 3.5 million social security numbers, 380,000 credit and debit card numbers, and the tax records of more than 650,000 businesses. In these two cases, for a customer or employee whose data has been stolen, these individuals must show that the stolen data had been used to the their financial detriment [30]. However, some courts hold that companies may be liable for damages if client or employee data is stolen, even if the theft causes no

harm [31]. In Korea, many cases have shown that customers may be actually held liable even if they file lawsuits for information leakage caused by hacking.

Third, the liability issue also tends to be slightly different according to the application areas. In the case of electronic card systems, some countries, such as England and Germany, seemingly assume the existence of gross negligence, which implies that the card holder must prove the absence of gross negligence [32]. However, others, including Belgium, do not assume the existence of gross negligence on the part of the customer, and state that the bank should prove that the customer was grossly negligent. In contrast to European countries, in the United States it seems to be irrelevant whether the card holder acted with extreme negligence or not when it comes to allocating liability. In the United States, the user's liability seems to depend on the time frame within which the holder notified his institution of the loss or theft of the instrument [32–34]. The Electronic Funds Transfer Act and Regulation E of the United States Truth in Lending Act contain a liability regime that favors the card holder. If notification has taken place within 2 days, the holder of a credit card can no longer be held liable. For transactions that have taken place prior to notification, the liability of the holder is always limited to 50 USD. If the consumer fails to report within 60 days, they will be liable for all transactions that have occurred after this period [32].

However, in the case of cryptocurrency, the liability tends to lie with the customer. According to a recent report from CipherTrace, hackers stole $927 million from cryptocurrency exchanges and other platforms in the first nine months of 2018, and the total damage was predicted to be $1 billion by the end of 2018 [35]. Recently, in Korea, the court decided that a customer should be held liable for damages even if the account had been hacked and the cryptocurrency had been stolen. The court did not rule in favor of the plaintiff in a lawsuit filed against a virtual currency exchange for "repayment of $50,000" (The judgment number: 2017gadan5016023). If the exchange is hacked but there is no obvious error on the part of the exchange, the exchange is not obligated to compensate the loss. On the other hand, if the exchange has not properly implemented security measures, the exchange shall be liable for damages due to breach. However, it is very difficult for the customers to prove that the exchange has not fulfilled its obligations. In summary, liability is closely related to the burden of proof, and it's not easy for customers to obtain damages due to security failure on the part of the exchange.

Table 4 shows the representative security breach cases with analytical results, such that customers (firms) take responsibility if the amount of damage caused by electronic transactions and the probability of an incident are small (large).

Table 4. Representative Cases of Security Breach with Analytical Results.

	Low m.	**High m**
Low ϕ or r	Customer's liability (when $\theta = \phi$): e.g., access control related to log-in process Identity theft (eBay), Credit card numbers theft (Trustwave Holdings)	
	Customer's liability (when $\theta < \phi$): e.g., access control related to log-in process, online fraud transactions	Firm's liability (when $\theta < \phi$): e.g., Software vulnerabilities, third-party integrations
High ϕ or r	Customer's liability: e.g., access control in cryptocurrency, mobile transactions	Firm's liability: e.g., credit card transactions in banking system (Target), data breaches in Facebook, Yahoo, and others

For a general privacy breach, such as identity theft at the access control level, customers seem to be held liable. In Korea, more than 6 billion pieces of personal information were leaked between 2007 and 2017 or used without permission. Even if some customers filed lawsuits for information leakage caused by hacking, the court did not recognize the liability of the firm for the most part, and consequently customers are actually held liable. Although the court recognizes the liability of the firm, penalties for personal information infringement incidents are very low. The analytical results in Table 4 implies that this can be the case when customers feel less privacy costs, or the relative size of

the 'risk averse' group is small. However, recent liability rules tend to shift from customers to firms. For example, two cases in the USA show that customers were held liable in 2015, while a recent case in 2018 showed that a firm has liability. According to Javelin Strategy and Research (2018), nearly 60 million Americans have been affected by identity theft and the United States government plans to spend $15 billion on cyber security for fiscal year 2019, which is a 4 percent increase over the previous year [36].

In particular, in Europe, the punitive damages can be very large if information leakage occurs. According to the Wall Street Journal, Facebook could be fined as much as $1.63 billion by a European Union privacy watchdog for a data breach in which hackers compromised the accounts of more than 50 million users, if regulators find the company violated the European Union's General Data Protection Regulation (GDPR) [36]. Yahoo also suffered a larger data breach in 2013 affecting 1bn accounts, and has been fined £250,000 for a hack that affected more than 515,000 UK email accounts that were co-branded as Sky and Yahoo services in the UK [37]. Such data breaches frequently happen in companies such as eBay, TJX Companies, Inc., Uber, JP Morgan Chase, Sony's PlayStation Network, Home Depot, Adobe, and many others [5]. In 2018, such data breaches also happened in companies such as Panera (37 million records), Under Armor (150 million records), and Facebook (at least 87 million records) [38].

Recent Facebook's failures in ensuring privacy for user data shows how important privacy and security assurance is for electronic transactions. As was mentioned previously, online fraud is becoming another major hindrance to the development and use of commercial activities on the Internet [4]. Customers frequently suffer damage from online fraud transactions in general ecommerce sites and travel sites.

In particular, customers using mobile devices in performing transactions, such as electronic banking, and mobile payments, need to insure against damage caused by hacking or fraud with regard to mobile transactions. This implies that customers could be held liable because the probability of a security breach can be higher in mobile transactions. Table 4 shows that if the probability of a security breach is high, customers may be responsible for the loss. Also, the liability issue can be discussed according to the stages of vulnerabilities in simple mobile transactions [21]. First, in the stage between the client and the mobile device, possession and ownership issues with regard to liability may occur. The ownership of a mobile device can become an issue if an unauthorized person is able to masquerade as the true owner, and engage in a transaction by assuming the identity of the owner. Second, in the stage between the mobile device and the mobile infrastructure operator, the liability seems to be detached from either the bank or the customer because transactions occur between the base station operated by a service operator and not within the business model of the bank engaged in the transaction. Many incidents, such as the introduction of malicious viruses, occur at this stage, and customers have had losses from such security breaches. A masquerade may be used to gain access to confidential information stored in a mobile device, modify the content of a transaction leading to financial loss, or introduce malicious codes (e.g., a Trojan horse). For this stage, there are not many specific liability guidelines, even though many security breaches can occur. Third, in the stage between the mobile infrastructure operator and the wireless application gateway of the bank, transactions occur in the network of the service operator. Although neither the bank nor the customer, generally, has any control over the network or the manner in which data is transmitted over the network, the bank should be concerned with protecting their information assets, as it is their responsibility. Last, in the stage between the wireless application gateway and the web services of the bank, the mobile transaction is likely to be under the control of the bank engaged in the transaction. Therefore, it may be beneficial for the bank to adopt liability guidelines and prepare security strategies to cope with specific security breaches, and to improve the trustworthiness of mobile transactions.

Liability allocation seems to differ according to areas. When a dispute regarding financial transactions arises between a bank and a customer, the burden of proof is imposed on the bank in the United States, which implies that the firm tends to have liability. This is supported by Chun et al. [27],

who show that in a market in which investments in security are highly effective, a legal regime can impose liability on the firm. However, in a dispute regarding cryptocurrency, the liability tends to lie with the customer. Table 4 explains the case regarding cryptocurrency. In the first half of 2018, $1.1 billion worth of cryptocurrency was stolen. This implies that the probability of a security breach can be higher in the case of cryptocurrency, and customers must be concerned about their security.

5. Conclusions

This paper analyzed the liability rule for e-business transactions when security or privacy breaches occur in online transactions. Although security and privacy issues are important factors with regard to browsing content on social media websites, several studies, including Mikalef et al. [7,39], have not considered these factors. Also, liability issues remain a major challenge to information security, and the components of human trust and security technology are regarded as important aspects of the cost involved in establishing trust in mobile transactions. However, previous studies have not stressed these issues and they have focused on technical factors, such as installing firewalls and intrusion detection systems, monitoring security alerts, and promptly implementing security patches. Thus, this paper investigates a liability rule for e-business transactions when security or privacy breaches occur in online transactions, considering both sides—the customer and the firm—and discusses how the liability rule can be applied to mobile payments and fraudulent e-commerce transactions. The results and implications are summarized as follows:

Firstly, if the amount of damage caused by electronic transactions and the probability of an incident is small, it is desirable for customers to take responsibility for social welfare. In practice, customers suffer losses from fraud transactions in many electronic commerce situations, including travel sites, because of the need to provide proof that they have no faults. Although, recent liability rules regarding privacy tends to shift liability from customers to firms, customers are liable for losses in cases such as identity theft at the access control level. Also, customers may be held liable regarding cryptocurrencies and must concern themselves with their own security when the probability of a security breach is high. However, this paper suggests that the firm may be liable for a loss if more customers are concerned about their security from a social welfare perspective. Secondly, if more customers are concerned with their security and with privacy risks, the regulatory regime assigns liability to the firm. When a dispute regarding financial transactions arises between a customer and a firm, a legal regime can impose liability on the firm in order to induce the firm to invest more in security or privacy protection. Thirdly, the investment model suggests that in a market where investments of the firm in security are highly effective, a legal regime can impose liability on the firm, even in the case where risk costs are lower, because a firm has a great deal of knowledge with regard to security technology and its investment efficiency can be high. Fourthly, this paper shows that a government may regulate a firm's price or subsidize a firm and impose liability on the firm if the probability of a security breach and customer losses are large. Lastly, if the probability of a security breach is high, and customers feel less loss, customers may be held responsible for the loss. However, if more customers are worried about loss, the government may involve and subsidize firms or customers with regard to insuring against damage caused by hacking or fraud with regard to mobile transactions.

This paper also has a number of limitations in that more cases regarding mobile transactions need to be analyzed because mobile transactions are rapidly increasing. In addition, the allocation of liability can also depend on customers' attitude towards risk when security or privacy breaches occur. Thus, in future work, liability with regard to mobile transactions needs to be investigated in terms of each participant when disputes occur with regard to different network levels.

Acknowledgments: This study is supported by the LG Yonam Research Foundation 2012.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Patton, M.A.; Jøsang, A. Technologies for Trust in Electronic Commerce. *Electron. Commer. Res.* **2004**, *4*, 9–21. [CrossRef]
2. U.S. Online Retail Sales Will Reach $459 Billion This Year. Available online: https://www.forrester.com/US+Online+Retail+Sales+Will+Reach+459+Billion+This+Year/-/E-PRE10039 (accessed on 22 January 2019).
3. U.S. Mobile Retail Commerce Sales as Percentage of Retail E-Commerce Sales from 2017 to 2021. Available online: https://www.statista.com/statistics/249863/us-mobile-retail-commerce-sales-as-percentage-of-e-commerce-sales (accessed on 21 January 2019).
4. Smartphone Volumes Expected to Rebound in 2017 with a Five-Year Growth Rate of 3.8%, Driving Annual Shipments to 1.53 Billion by 2021, According to IDC. Available online: https://www.businesswire.com/news/home/20170301005212/en/Smartphone-Volumes-Expected-Rebound-2017-Five-Year-Growth (accessed on 21 January 2019).
5. Alhabash, S.; Ma, M. A Tale of Four Platforms: Motivations and Uses of Facebook, Twitter, Instagram, and Snapchat among College Students? *Soc. Media Soc.* **2017**. [CrossRef]
6. News Use across Social Media Platforms 2018. Available online: http://www.journalism.org/2018/09/10/news-use-across-social-media-platforms-2018 (accessed on 22 January 2019).
7. Mikalef, P.; Giannakos, M.; Pateli, A. Shopping and word-of-mouth intentions on social media. *J. Theor. Appl. Electron. Comer. Res.* **2013**, *8*, 17–34. [CrossRef]
8. Cybersecurity Ventures Sponsored by Herjavec Group. Cybercrime Damages Will Cost the World $6 Trillion Annually by 2021. 2017. Available online: https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf (accessed on 21 January 2019).
9. The 18 Biggest Data Breaches of the 21st Century. Available online: https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html (accessed on 21 January 2019).
10. $1.1 Billion in Cryptocurrency Has Been Stolen This Year, And It Was Apparently Easy to Do. Available online: https://www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-do.html (accessed on 22 January 2019).
11. Gavish, B.; Tucci, C.L. Fraudulent auctions on the Internet. *Electron. Commer. Res.* **2006**, *6*, 127–140. [CrossRef]
12. Leavitt, N. Mobile Security: Finally a Serious Problem? *Computer* **2011**, *44*, 11–14. [CrossRef]
13. Marous, J. The Future of Mobile Banking: Market Shift or Market Growth? Available online: https://thefinancialbrand.com/60418/fed-mobile-banking-payments-usage-study/ (accessed on 22 January 2019).
14. Research, J.S. More Than 12 Million Identity Fraud Victims in 2012 According to Latest Javelin Strategy & Research Report. Available online: https://www.javelinstrategy.com/press-release/more-12-million-identity-fraud-victims-2012-according-latest-javelin-strategy-research (accessed on 21 January 2019).
15. Mobile Banking: Safe, at Least for Now. Available online: https://www.cnet.com/news/mobile-banking-safe-at-least-for-now/ (accessed on 22 January 2019).
16. Kleist, V.F. A Transaction Cost Model of Electronic Trust: Transactional Return, Incentives for Network Security and Optimal Risk in the Digital Economy. *Electron. Commer. Res.* **2004**, *4*, 41–57. [CrossRef]
17. Kim, H.; Han, Y.; Kim, S.; Choi, M. A Curriculum Design for E-commerce Security. *J. Inf. Syst. Educ.* **2005**, *16*, 10.
18. Niranjanamurthy, M.; Kavyashree, N.; Jagannath, S.; Bhargava, R. M-commerce: Security challenges issues and recommended secure payment method. *Int. J. Manag. IT Eng.* **2012**, *2*, 374–393.
19. Horn, G.; Schneider, P. Towards 5G Security. In Proceedings of the 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-15), Helsinki, Finland, 20–22 August 2015; pp. 1165–1170. Available online: https://ecfsapi.fcc.gov/file/60001520704.pdf (accessed on 22 January 2019).
20. Munisankaraiah, S.; Kumar, A.A. Physical layer security in 5G wireless networks for data protection. In Proceedings of the 2016 2nd International Conference on Next Generation Computing Technologies (NGCT), Dehradun, India, 14–16 October 2016; pp. 883–887.
21. Misra, S.K.; Wickamasinghe, N. Security of a Mobile Transaction: A Trust Model. *Electron. Commer. Res.* **2004**, *4*, 359–372. [CrossRef]
22. Nilmini Wickramasinghe, S.G. M-Health: A new paradigm for mobilizing healthcare delivery. In *Unwired Business: Cases in Mobile Business*; IGI Global: Hershey, PA, USA, 2005; pp. 187–204.

23. Angelakopoulos, G.; Mihiotis, A. E-banking: Challenges and opportunities in the Greek banking sector. *Electron. Commer. Res.* **2011**, *11*, 297–319. [CrossRef]
24. Dahlberg, T.; Mallat, N.; Ondrus, J.; Zmijewska, A. Past, present and future of mobile payments research: A literature review. *Electron. Commer. Res. Appl.* **2008**, *7*, 165–181. [CrossRef]
25. Chun, S.-H.; Rhee, B.-D.; Park, S.Y.; Kim, J.-C. Emerging dual channel system and manufacturer's direct retail channel strategy. *Int. Rev. Econ. Financ.* **2011**, *20*, 812–825. [CrossRef]
26. Chun, S.-H.; Ko, Y.-W. Security and Liability in a Smart Mobile Environment. *Int. J. Urban Des. Ubiquitous Comput.* **2017**, *5*, 27–32. [CrossRef]
27. Chun, S.-H.; Cho, W.; Subramanyam, R. Transaction security investments in online marketplaces: An analytical examination of financial liabilities. *Dec. Support Syst.* **2016**, *92*, 91–102. [CrossRef]
28. If My Website Is Hacked and Customer Data Exposed, Am I Liable? Available online: https://smallbiztrends.com/2016/07/website-hacked-customer-data-exposed-liable.html (accessed on 21 January 2019).
29. What Is GDPR? The Summary Guide to GDPR Compliance in the UK. Available online: https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018 (accessed on 21 January 2019).
30. Courts Restrict Ability of Customers and Employees to Sue Companies Following a Data Breach, but Risks of Other Liabilities Remain. Available online: https://www.workplaceprivacyreport.com/2015/06/articles/written-information-security-program/courts-restrict-ability-of-customers-and-employees-to-sue-companies-following-a-data-breach-but-risks-of-other-liabilities-remain (accessed on 22 January 2019).
31. If You're Hacked, What's Your Cybersecurity Liability? Available online: https://blog.aicpa.org/2017/10/if-youre-hacked-whats-your-cybersecurity-liability.html#sthash.UHynor80.dpbs (accessed on 22 January 2019).
32. Steennot, R. Allocation of liability in case of fraudulent use of an electronic payment instrument: The new Directive on payment services in the internal market. *Comput. Law Secur. Rev.* **2008**, *24*, 555–561. [CrossRef]
33. Hance, O.; Balz, S.D. *The New Virtual Money: Law and Practice*; Kluwer: London, UK, 1999.
34. Vartanian, T.P.; Ledig, R.H.; Bruneau, L. *21st Century Money, Banking and Commerce*; Fried, Frank, Harris, Shriver & Jacobson: Washington, DC, USA, 1998.
35. Nearly $1 Billion Stolen In Crypto Hacks So Far This Year: Research. Available online: https://www.coindesk.com/nearly-1-billion-stolen-in-crypto-hacks-so-far-this-year-research (accessed on 21 January 2019).
36. Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017. Available online: https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin (accessed on 23 January 2019).
37. Yahoo Fined £250,000 for Hack That Impacted 515,000 UK Accounts. Available online: https://www.theguardian.com/technology/2018/jun/12/yahoo-fined-hack-ico-uk-accounts-russia (accessed on 22 January 2019).
38. Facebook Faces Potential $1.63 Billion Fine in Europe over Data Breach. Available online: https://www.wsj.com/articles/facebook-faces-potential-1-63-billion-fine-in-europe-over-data-breach-1538330906 (accessed on 22 January 2019).
39. Mikalef, P.; Giannakos, M.; Pateli, A. Exploring the Business Potential of Social Media: An Utilitarian and Hedonic Motivation Approach. In Proceedings of the 25th Bled eConference eDependability: Reliable and Trustworthy eStructures, eProcesses, eOperations and eServices for the Future, Bled, Slovenia, 17–20 June 2012.