2010

OPTIMAL ONLINE BANKING SECURITY CONFIGURATION UNDER BURDEN OF PROOF

Myunsoo Kim
KAIST Business School, jamaica@business.kaist.ac.kr

Byungtae Lee
KAIST Business School, btlee@business.kaist.ac.kr

OPTIMAL ONLINE BANKING SECURITY CONFIGURATION UNDER BURDEN OF PROOF

Completed Research Paper

Myunsoo Kim
KAIST Business School
87 Huegiro Dongdaemoon-gu Seoul, Korea
jamaica@business.kaist.ac.kr

Byungtae Lee
KAIST Business School
87 Huegiro Dongdaemoon-gu Seoul, Korea
btlee@business.kaist.ac.kr

Abstract

Against the threat of online banking theft, governments are imposing two different types of legal schemes: strict liability and negligence. Countries like the U.S. are imposing strict liability on online banking transactions to ensure that service providers like banks take more care. However, under strict liability banks does not provide adequate client security measures. Countries like Korea are imposing burden of proof on online banking transactions to ensure that general public take more care and reduce burden of accident prevention on banks. However, under burden of proof service providers are developing and providing excessive number of client security measures for their users. In each legal regime online banking security configurations are not consistent with the original intention of the related liability scheme. This paper investigates using microeconomic models how unique characteristics of information technology changed traditional working mechanism of the liability scheme with microeconomic models and it also provides practical implications for managers.

Keywords: Online banking, security, burden of proof, strict liability, information technology

Introduction

Information and communication technology enables everyday online banking transactions. With a personal computer hooked up to the internet, anybody can make money transactions whenever and wherever they are. This new money transaction method, i.e. online banking, is popular and its use is increasing. The total number of active online banking customers reached 47 million in the U.S. in 2008, and additionally more than 30% of all banking transactions were internet based.[1]

However, there exists a downside of online banking. Online theft is also dramatically increasing, with a total of 656 cases as of the end of 2008. It showed an increase of 47% in the US in 2007.[2] And the threat of online theft is recognized as a major barrier to online banking adoption (Suh and Han, 2002). A cyber thief will try to break or fool installed security measures and transfer an innocent user's money to the thief's account so he might withdraw it as cash. One of the most popular methods is called 'stolen identity'. A thief will install key-logging software on the victim's personal computer, which records every key stroke the victim enters in his/her computer including online banking passwords, and send that information to a designated location (most probably the thief's computer). Then, the thief will receive the victim's online banking password and using this information he/she can log into the online banking system with the stolen identity, and will be able to transfer the victim's money into his/her own account.

Unlike old ATM systems based on host-terminal architecture, new online banking is mostly based on the server-client architecture. A personal device and an internet connection are essential to online banking transactions. The bank's computer is working as a server and all users' personal units are working as clients, and both server and clients are connected via internet. A cyber thief can attack either server or client, or even both. A bank, which is generally a large organization, usually hires proper security experts to deal with such attacks. Unfortunately, when it comes to the client situation, properly maintained security is not easily achieved. To protect a client's personal computer, a proper set of security measures is needed. Such security measures include anti-keylogger programs, digital signage encryption methods, one-time passwords and otherwise similar methods. However, developing and applying such security measures needs a lot of computer related experience, and the general online banking users do not have such extensive knowledge about computer security. Users are not in a good position to identify which security measures are needed, let alone developing them. Hence, the general user's client personal computer is an easy target, and for such reasons is often targeted by online banking thieves (Beak, 2006).

Computer scientists have researched the subject of how to improve the client personal computer's protection (Claessens, 2002) and many business related papers brought up its impact on business strategy (White, 2008). However, very few have looked the legal side effects and their related implications. Since a user owned personal computer is essential for online banking, a simple question must be answered: who is responsible for the damage if an attack on the client's personal computer was successful? The law must be involved to answer such a question. There are two different liability schemes that are applicable to the matter: *strict liability* and *negligence*.

Some countries like the United States (regime 1 hereafter) impose a strict liability scheme (i.e. product liability) in which a bank will immediately compensate the victim for any damage caused by electronic transactions[3]. The idea of strict liability is that a firm is in a better position to prevent accidents (Cooter, 2004). Therefore it is cheaper if the firm embraces all the responsibility and reduces the cost from it by according to the economy of scale. A good example would be a lawnmower equipped with a safety handle. It is obviously cheaper if the safety handle is mass produced by the production company itself, than if every customer makes their own safety handle in their own garage. Under strict liability, banks should receive more incentives for developing and providing client security measures, as they have full responsibility.

On the other hand, in countries like the Republic of Korea (regime 2 hereafter), in order for a customer to get proper reimbursement from any fraudulent transaction, the related law requires proof that the user was not grossly negligent during the online banking transaction[4]. This is a typical negligence liability scheme and is based on the idea that

[1] comScore State of Online Banking. http://www.comscore.com/request/state_of_online_banking.asp

[2] Identity Theft Resource Center, 2009.

[3] Federal Reserve Board's Regulation E: http://www.federalreserve.gov/bankinforeg/regecg.htm

[4] Korean electronic commerce law, article 9

both parties (in this case, the user and the bank) must take appropriate care to prevent any accidents (Cooter, 2004). A good example would be a traffic accident. Any involved party should have been careful to prevent an accident. If anyone of these parties cannot prove that it took proper care, then that party must bear full responsibility for the entire damage of the accident. A bank in regime 2 has a relatively better chance to escape from liabilities than a bank in regime 1. This should lead to relatively less strict prevention measures on the bank side and to an increased level of care on the user's side, which inevitably leads to increased cost requirements to the user.

It is very interesting that banks do *not* seem to fulfill the obligations expected from each liability scheme. Banks in regime 1 do not explicitly provide any viable client security measures, for there are worries such as "as some consumers are finding out the hard way, only a username and password stands between criminals and their hard-earned money."[5] In regime 2 there are ongoing debates about excessive client side security measures that are required for a simple online transaction – most websites require at least 4 preinstalled security measures.[6] The strict liability scheme in regime1 should have forced banks to protect their clients' personal computers more aggressively, however currently virtually no client security measures are provided. Also the negligence liability scheme in regime 2 should have the effect of urging online banking users to take additional care, and of reducing the burden of responsibility from the banks. However banks are providing too many client security measures than the users want.

Normal technological or traditional law and economics perspectives are not enough to fully explain such a seemingly contradictory phenomenon. We suspect that the unique characteristics from information technology, such as client-server architecture, software, and the internet have distorted the original intent of those legal schemes. Considering characteristics of information technology, we will explain this seemingly contradictory phenomenon with a simple microeconomics model.

Another issue is 'blame shifting'. There is an ongoing debate that software companies and online service providers tend to shift the blame to internet users as a last resort. They either force users to take full responsibility through End User License Agreements or let them handle sensitive processes for themselves (Anderson, 1994). Anderson suggested that liability can be transferred to a 3rd party or even to the customers. For example, a software vendor could provide their latest upgrade to internet users without any charge, and the user would only have to download and install it. Or the vendor could provide it for a substantial fee. Most users save money by installing the upgrades themselves – and in doing so lose much of their rights to sue the vendor if their files get corrupted. If we apply the idea of blame shifting to online banking, a bank in regime 2 could hide its intention of shift blaming by disguising it as a good will: "You will become safer with our newly developed client security measure". The bank faces the choice of how to shift blame and how much security is optimal for them. We will provide a model to explain under what conditions the bank will shift blame to its users. For this end, the following specific research questions are addressed.

The first research question is: Why were online banking security configurations developed in the opposite directions that were intended in each legal schema? The client security measures in online banking are not being configured as the legal scheme intended. We will show that characteristics of information technology have caused banks to deviate from what laws and economics models suggest, and this has resulted in unintended security configurations. Second: under what conditions will banks try to shift blame to their customers via client security measures? In regime 2, banks and governments are continuously increasing mandatory client security measures for online banking transactions, "for the users own safety." However, we will show that under the negligence liability scheme which involves burden of proof that the bank has enough incentives to provide more client security measures than the users actually want, if those client security measures create enough burden of proof assigned to its users. The final research question is: Can a bank of one legal scheme use strategies from banks of the other legal scheme? Banks under different legal schemes are using totally different strategies that seem to be incompatible. With our suggested model and implications, managers can identify the relative competitiveness and utilize it in different liability schemes.

In section 2, we will review previous studies and define how we will take our approach to address the aforementioned research questions. In section 3, we present a basic model to describe client security measures and their legal side effects in the case of regime 1, which explain why banks are reluctant to provide client security measures under strict liability. In the ensuing section, we show that in regime 2, banks will more aggressively

[5] Bob Sullivan, Online bank fraud concerns consumers, MSNBC, 2004.

[6] Openweb suit, http://openweb.or.kr/?p=1329

provide client security measures that clearly differ from regime 1. Finally in section 5, managerial and policy implications for banks and governments are discussed along with limitations and possible future research directions of this study.

Literature Review

There have been ongoing debates about changes from negligence to strict liability or whether product liability is economically efficient or not. Since 1940, it is widely accepted that product liability is better when (1) manufacturers have market power, which allows them to dictate unfair terms in warranties and underinvestment in product-safety technology, (2) manufacturers are better placed than consumers are to spread the losses from product related injuries, (3) manufacturers are better placed than consumers are to minimize the losses from product accidents by taking precaution and improving technology (Cooter, 1994). However, only after several decades, Priest (1985) claimed that first two of these premises are wrong. Therefore hasty movement to enterprise liability may be based on misled rationales. On the other hand, Landes and Posner (1985) suggested that product liability is, in general, efficient.

In online banking, attempts to steal a victim's identity are generally done using Trojan horses type malware. It is virtually impossible to bring the creator of specific malware into the court. In fact, it is very hard to even identify which malware did the job for the thief. Moreover, with an economic perspective, online theft or identity theft has significant effect on social dimension (Singh, 2006). Awe on online theft works as a barrier in online banking adoption (Suh and Han, 2002), for security issue is a major deterrent to user acceptance of online banking (Wang, 2003). A disturbing report about why online banking users are not increasing as forecasted, points also at securities (White, 2004). Although these studies linked security performances and entry barriers for using online banking, it is still unclear how much costs to users can be attributed to the lack of security performances.

In addition, who should take the burden or the risk, is still in debate. McCullagh (2005) suggested a user must weigh both risk of online theft and benefits from convenience. In regime 2, as a bank's responsibility for this matter has dramatically increased over the last few years, now there is a debate regarding its effectiveness from economic perspective (Jung, 2005). Technologically there is also a critical issue regarding online privacy. Shumaila (2003) suggested that in order to create e-trust in electronic banking, both parties must be somehow informed of the history of transactions. However the more the information goes through online, the more increases the risk that online thefts may take place (Caudill, 2000). This can be even trickier when dealing with international transactions, which involves different liability schemes (Miller, 2002).

Anderson (1994) also suggested, in regime 1 with strict liabilities, banks are offered fewer incentives to develop effective security measures, for they are not worthy. While in regime 2 a user must install numerous client security measures already, banks and government agencies suggest that users must adopt more security measures in order to prevent online theft. Although these studies aimed on explaining risk and benefits of security measures, and responsibility of trading parties, it is still not clear what burden of proof or cost of care goes to whom, or how those cost are created and transferred. These issues have been widely studied in legal realms but not specifically under information security context. In addition, we already explained that market outcomes seem to be grossly deviated from what laws and economic theories have suggested in liability schemes for general trades. We try to fill this void.

Furthermore, security measures are not the only things that evolve. Evolution in malware means the law must have more technological insights.

Due to increasing uses for stolen identities, and the recent revolution of botnet, Malware attacks on personal computers are increasing more than ever. If a malware operates in server computers of banks, it would be a bank's problem. On the contrary, if a malware operates on the user's computer, the issue becomes dramatically complex and unsettled. If we subscribe to product liability, users are certainly not in a better position to find out with what or how they should protect their own financial transactions and assets which lie in the bank server. This means government or banks ought to invest more to reduce the user's burden, especially when strict liability is not applied. Baek (2006) suggested that the Korean government and banks must adopt a new method to deal with this problem other than just increasing the amount of traditional security software.

Clearly legal schemes may have strong influence how banks and governments should behave so that they also have impact on banks' profit and social welfare. The ensuing sections illustrate them.

Regime 1 under Strict Liability

Basic Model

Law and economics have suggested many microeconomic models on liability issues. We incorporate information technology characteristics into our model based on the skeleton of those models.

A bank is providing online banking service for many users. Each user requires online money transfer with a certain transaction size s, which is uniformly distributed over [0, 1]. A bank will receive a fixed fee f from users for each transaction. The fee is set at the market price. Any online transaction will face the threat of online theft, with probability of p_0, $0 < p_0 < 1$. The thief steals the money if the attack succeeds. Hence, without any post accident legal protection, a user's expected damage is $p_0 s$.

The probability of theft will be lowered if one or both parties take some level of care to prevent the theft. Let p_m be the probability of theft with adequate security measures. Since we assume that those measures are somewhat effective, p_m is assumed to be smaller than p_0.

Online banking is based on server-client architecture, both server and client must be protected from possible theft attempts. This is clearly different from the old ATM system which is based on host-terminal architecture. With the ATM system, both host and terminal are under the bank's responsibility. However, with online banking, the client's computer is under the user's responsibility and ownership. In order to achieve the lower probability of theft p_m, both user and bank must exercise due care to protect the client and server, respectively. The required level of care to achieve p_m, should be the total sum of both parties' level of care. Now let x be the level of care for a user, then that of the bank is $1-x$. It is clear that both parties will try to shift the responsibility to each other under the assumption that additional care always incurs more costs.

However, a user is clearly in the worse position to decide the level of care, x. In online banking, the user's level of care can be translated to the number of software client security measures he or she uses to protect his/her own computer. It is assumed that each individual user is virtually unable to develop proper client security measures with their own means, partially due to the lack of expertise or the lack of information on server-side programs[7]. Hence, banks should determine a set of security measures and enforce them. Higher security measures may have software applications which may be downloaded via internet with virtually no cost to banks in copying and distributing client security measures (Shapiro, 1999). This means that banks decide x and make those available to its users. The online banking transaction will not work unless the user accepts the entire set of client security measures required by the bank. Unlike a typical tort situation of other physical goods, online banking users cannot decide their level of care. The user can only decide whether to use the recommended client security measure or not: "take it or leave it". If a user decides not to accept the required client security measures, a user does online transaction with the higher probability of p_0

Cost of Care

Cost of care means the cost incurred by taking a certain level of care. With online banking, a user must install and activate provided client security measures. Installation requires waiting time, activation also requires waiting time and at least additional clicks even for the password, in some cases even additional independent passwords. Time and resources can be considered as the user's cost of care c, $0 < c < 1$, incurred by client security measures.

The bank which we assume to be large enough to carry out appropriate measures already bought and maintains large scale computer related security services. Hence the marginal cost of care for any additional transaction is negligible. And since we are focusing on relatively short term behavior, the fixed cost is sunk and can be ignored.

---

[7] The user can use commercial security measures from 3rd party security software vendors. However if the 3rd party security measures are not certified by the bank, the user cannot be sure that they will work for the various kinds of online theft or not. Therefore, as long as the security measures from the bank are free, there is no need to use uncertified security measure from other sources.

Let's assume that the bank offers client security measures while other competitors do not. Let s be the normalized transaction size of a typical customer of the bank with security measures (i.e. $s \in [0, 1]$). A user can choose this bank or one without security measures. The expected profit functions with the bank and any other become (1) and (2) where f is the transaction fee at the competitive market price.

$$\pi_u = -f - p_m \cdot s - c \tag{1}$$

$$\pi_u = -f - p_0 \cdot s \tag{2}$$

Obviously, the magnitude of c and the effectiveness of security measures decide the balance between the two cases. Hence, banks with security and without may co-exist in the market. However, in the following subsection we show that no bank will try to provide security measures first under a strict liability scheme.

Strict Liability

In the case of Judd vs. Citibank (Anderson, 1994, pp.6-7), Citibank claimed that their system was infallible, which the jury found out not to be true. Since then, for any U.S. customer who loses money over electronic transactions, the bank must refund fully the losses fully minus $50. Reg-E, or the Federal Reserve Board's Regulation E[8] was established under the Electronic Funds Transfer Act of 1979. This covers situations that any access devices such debit card or online banking password is lost, consumer liability is capped for $50 under the conditions that the customer notifies the bank within two business days since he/she recognizes the lost. Consumers who notify the bank within 60 days have their liability capped at $500. After 60 days, any damage which occurred becomes the consumers' responsibility. On the other hand, if no access device is lost, and fraudulent charges mysteriously appear on a consumer's account, the liability clock begins when the bank notifies its customer of the activity, usually through regular monthly statements. Banks must investigate disputed charges within 10 days, and report results to the consumer within three days. Errors must be fixed within one day. If the investigation cannot be completed within 10 days, banks must issue a provisional credit to the consumer for the disputed amount, less $50. The user has no responsibility whatsoever to take preventative actions.

Analysis

Under strict liability, the bank will compensate any damage done to the user immediately and that banks are not required to achieve p_m because general public is already protected by unconditional post-accident compensation. This changes user's profit functions dramatically. Now let us consider the case when our bank is trying to develop and provide client side security measures under strict liability. The liability scheme is affecting all banks in the regime. We will ignore the refund fee since we are focusing on the user's cost induced by legal schema. Eq. (1) and eq. (2) becomes (3) and (4) respectively.

$$\pi_u = -f - c \tag{3}$$

$$\pi_u = -f \tag{4}$$

No user will use the bank with client security measures (CSM) due to induced cost of care. And any bank must pay all incurred damage to customers. The bank which enforces CSM has its expected profit function:

$$\pi_b = f - \int_0^1 p_m \cdot s ds = f - \frac{1}{2} p_m \tag{5}$$

That of one without CSM is:

$$\pi_b = f - \int_0^1 p_0 \cdot s ds = f - \frac{1}{2} p_0 \tag{6}$$

[8] http://www.federalreserve.gov/bankinforeg/regecg.htm

A simple normal form game theory approach will show the above argument more clearly.

Table 1. Bank's Profit under Strict Liability		
The bank / The other	CSM	No CSM
CSM	$(f-\frac{1}{2}p_m\ ,\ f-\frac{1}{2}p_m\ )$	$(0,\ f-\frac{1}{2}p_0\ )$
No CSM	$(f-\frac{1}{2}p_0\ ,0)$	$(f-\frac{1}{2}p_0\ ,\ f-\frac{1}{2}p_0\ )$

Note that the bank with CSM will not have any customer in asymmetric cases in this game according to the aforementioned result from Equation (3) and (4).

While players will be better off when both banks provide CSM and it is also socially more desirable since $p_m < p_0$, no bank will try to do it "first", because of possible breach. This is a typical prisoner's dilemma working against social welfare, and only strong external incentives or regulations will solve this suboptimal equilibrium.

Proposition 1*: Under strict liability, online banking users will not accept services involving client security measure due to incurred cost of care as long as there are other services without cost of care.*

Now under strict liability no bank will try to provide client security measures. We find that banks employ other measures to mitigate the risk such as limiting transaction size. As of 2009, Citibank is restricting its size of transactions.[9] Domestic transactions are limited to $1000~$2000 per day. If we set maximum transaction size as a decision variable, it is easy to derive that the bank's profit is maximized when

$$\hat{s}_{strict} = \frac{f}{p_0} \tag{7}$$

Since bank's profit function is $\pi_b = fs - \int_0^s p_0 \cdot z dz$. And,

$$\hat{s}_{strict} < \frac{1}{2} \tag{8}$$

Proof is in Appendix A.

Regime 2 under Burden of Proof

Burden of Proof

Regime 2 invokes burden of proof, which usually states "banks are strictly liable unless the victim was grossly negligent"[10]. Also, the definition of gross negligence follows the rule of one or both of the following conditions: the victim lent particular access devices, including passwords; or the victim did not protect access devices even if the victim knew the risk of breach.[11] This type of liability scheme is more precisely categorized as strict liability with defense of contributory negligence (Cooter, 2004). The service provider, in this case the bank, will be strictly liable except when the victim was negligent. Government agencies insist that these conditions are only for extreme cases

[9] Citibank online: https://online.citibank.com/JRS/portal/template.do?ID=MoneyXfrCompare

[10] Korean electronic commerce law, article 9

[11] Korean electronic commerce law enforcement ordinance, article 8

therefore the burden of proof will be minimal. Indeed, this condition changed from "negligence" to "gross negligence" in the year 2006, further lowering the burden of proof.[12]

Some anecdotal evidence in regime 2 shed light on how financial institutes behave differently under this condition. Despite the government and consumer agencies efforts, Kookmin Bank, one of the major Korean retail banks, never compensated any victim for online theft during the years 2007 to 2008[13]. Kookmin Bank has been "waiting" for the official police investigation. There has been only one reported case of actual compensation of the damage from online thefts to the victims in Korea, by Korea Exchange Bank, another major retail bank. However, this bank claimed "we are not paying the victim because we are liable; we are paying because we value our customers."[14]

These delays or denials in victim compensation are clearly different from regime 1 cases. If strict liability is in effect, the victims get compensated almost immediately[15]. At least, it is safe to say in regime 2, burden of proof for the victim of online theft is practically in effect. Such facts bring questions about exactly how high this burden of proof should be.

It is obvious that online banking users with burden of proof have less protection from theft damage. The governments will try to protect the general public by reducing the probability theft. Hence, there tends to be more compliance requirements. For instance, in Korea (a typical case of regime 2), online banking transactions require digital signage, a pre-assigned key-code and even one-time-password (OTP) devices for larger transactions, in addition to basic anti-keylogger, anti-virus, anti-malware software. They are all required by laws. Hence, the lower probability of theft, p_m is somewhat imposed by society rather than an endogenous decision by the banks themselves. While it is possible for banks to optimize its probability level by adjusting investment levels on server side security measures, since they have easier and often cheaper alternative of changing x to users without incurring much cost, we assume that banks try to comply the exogenously imposed level p_m. Under this assumption, we investigate how many client security measures the bank must set to maximize its profit.

Burden of proof is typically modeled as a litigation cost. A user must pay litigation costs to prove that he was not grossly negligent. We will set the litigation cost as $k(x)$, and of course, $\frac{\partial k(x)}{\partial x} > 0$. For simplicity of analysis, let $k(x) = kx,\ 0<k<1$. When users are given multiple sets of security measures, they have to prove that none of given measures were executed without proper care. Hence, it will multiply users' burden of proof.

Still, if a user doesn't want to use the bank's services, the user may adopt some other solutions provided by 3rd parties like Paypal[16] . Since such solutions don't provide client security measures for user convenience, we ignore the cost of care and litigation cost of them in our model. In litigation, users using any other online transaction method other than our bank cannot be compensated in any way. The only way for a user to get compensation is if the user applies all the client security measures properly.

Analysis

Fixed Cost of Care

For simplicity, let us assume that the cost of care c is invariant with the number of client security measures x since each installation and activation of client security measures usually is an automated batch-job.

We will investigate the user's profit function along the user's online banking transaction size. Figure 1 shows how the user's expected cost or profit changes along the transaction size. The user can be categorized into one of the following 3 cases according to his/her transaction size.

---

[12] Digital Times, 2007, http://www.dt.co.kr/etc/article_print.html?article_no=2007053002011557729001

[13] NewsTomato, 2008, http://news.etomato.com/news/all_news/etomato_news_read.asp?no=6653

[14] MoneyToday, 2005, http://www.mt.co.kr/view/mtview.php?type=1&no=2005060718275075354

[15] http://www.federalreserve.gov/bankinforeg/regecg.htm

[16] Regime 2 countries like Korea have services similar to Paypal, which are not explicitly protected by the law: http://cafe.daum.net/soeaek

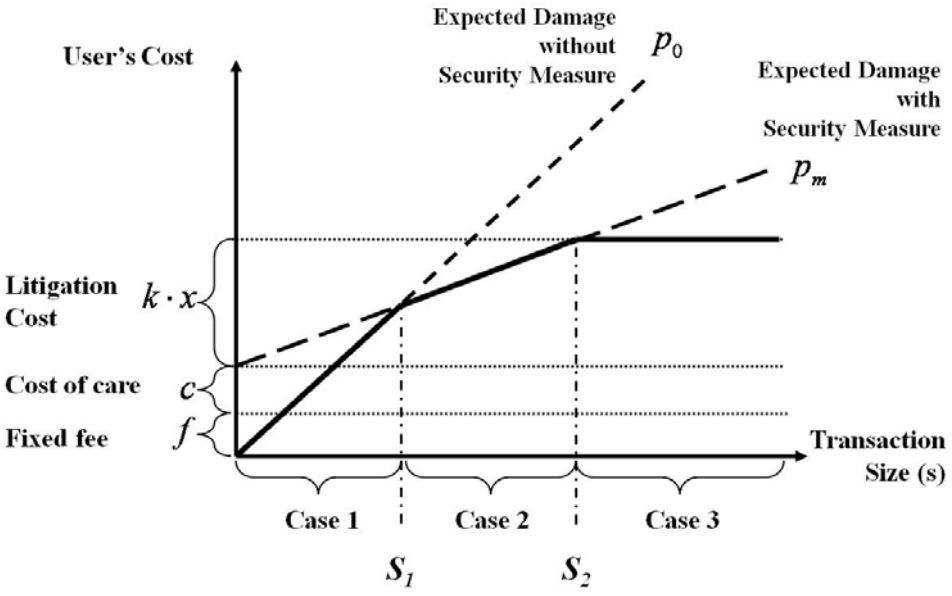

Figure 1. User's expected cost along the transaction size

Let $s_1 = \min\{s_C, s_L\}$ and $s_1 = \max\{s_C, s_L\}$ where $s_C = \dfrac{f+c}{p_0 - p_m}$ and $s_L = \dfrac{kx}{p_m}$.

Case 1 where $s < s_1$ (small transactions), Case 2 where $s_1 < s < s_2$ (medium transactions), and Case 3 where $s_2 < s$ (large transactions). The user's choices in the three cases are different.

In Case 1, the users do not adopt CSM as their transaction size is not worth the fee and the induced cost of care. While we model the monopoly bank, nowadays, there are many alternatives such as digital payments, cell phone payments, and electronic payment such as Paypal. Most of them are widely used for micro-transactions. Hence, when the bank enforces security measures, we assume that the users will leave the bank for alternatives. Users with the medium sized transactions will use CSM. However, due to litigation costs, these users would not sue the bank.[17] Clients with large transactions (Case 3) pay the fees, cost of care, and eventually litigation costs to get compensation when the damage occurs.

We can write the user's profit function in general form as following:

$$\pi_u = \max\{\underbrace{-f - p_0 \cdot s}_{\text{case1}}, \underbrace{-f - p_m \cdot s - c}_{\text{case2}}, \underbrace{-f - k \cdot x - c}_{\text{case3}}\} \tag{9}$$

The aggregated profit of all users becomes:

[17] We are assuming both parties pay their own litigation costs to see the effect of litigation cost more clearly. U.S. courts allocate legal fees to both parties, while most European courts state that the loser must pay all legal fees. Even if the court allocates the legal fees to the loser, the actual reallocation is done after the verdict, which could be take place after a very long time period. Hence, theoretically, when litigation cost can be recovered by winning, the expected cost of litigation can be lowered and the plaintiff will take consideration of winning probability. Therefore the winner still faces risks of temporal poverty (a type of opportunity cost), and these risks can be translated as the litigation cost. The scale parameter k reflects them.

$$\pi_{u,t} = -f - (1-s_1)c - \int_0^{s_1} p_0 \cdot s ds - \int_{s_1}^{s_2} p_m \cdot s ds - \int_{s_2}^{1} k \cdot x \cdot ds \tag{10}$$

Under regime 2, it is assumed that users will be fully compensated by courts when burden of proof is met. Then, the resulting profit of the bank becomes

$$\pi_b(x) = \underbrace{\int_{s_1}^{1} f \cdot ds}_{\text{Fee Income}} - \underbrace{\int_{s_2}^{1} p_m s \cdot ds}_{\text{Compensation Expenditure}} \tag{11}$$

$$\pi_b(x) = \left(1 - \frac{c+f}{(p_0 - p_m)}\right) - \frac{1}{2} p_m \left(1 - \frac{k^2 x^2}{p_m^2}\right) \tag{12}$$

It is self-evident that the bank's profit is maximized with the optimal allocation of users' share of CSM,

$$x_b^* = \frac{p_m}{k} \tag{13}$$

Note that with this optimal allocation, $\hat{s}_{burden} = s_L = s_2 = 1$, since determining *x* will automatically determine *s*. Hence, with this result, the following proposition is derived.

Proposition 2*: Under burden of proof and when the cost of care is fixed, the bank always assigns the unique optimal number of client security measures, and transaction size limit is set at the maximum.*

Let's assume that financial regulatory agency focuses only welfare of customers, and then it will try to maximize the aggregated surplus of bank users, defined in Equation (8). Then, we can easily show that $x_u^* = 0$ is the social optimal. The reason that the optimal is set at the corner solution is because the agency does not take account of welfare of banks but only the users. It is obviously the best to users when as much as costs were assigned to firms.

Both results are consistent with intuitional expectations. The bank will certainly try to minimize compensation, enforcing the maximum litigation cost to users. Since we capped user transaction size at 1, the bank will try to impose enough litigation cost on its users to avoid any compensation, by giving a large number of client security measures. With less litigation cost users have better chance to get compensation initiating litigations. Thus, bank's desirable number of client security measure is positive and much larger than the social optimal.

Since we are investigating bank's possible exploitation of litigation cost over online banking transactions, our monopolistic assumptions have simplified the analysis and helped to provide an understanding of the litigation cost transfer mechanism. As we have discussed in previous sections, in regime 2 banks are denying or at least delaying online theft victim's compensation, while users are complaining about the excessive number of client security measures. The analysis and implications are valuable in understanding such real world phenomenon.

Also, note that under regime 1 strict liability, optimal allowed transaction size was set as $\hat{s}_{strict} = \frac{f}{p_0} < \frac{1}{2}$, while under regime 2: burden of proof the bank will allow the maximum transaction size which is 1 when cost of care is fixed. Our findings predict that under burden of proof bank will allow far larger sized transactions than of a bank under strict liability. Reality coincides with our finding, for Kookmin Bank which is under regime 2 sets a far larger transaction size limit than Citibank[18]. The former's limit is $30,000 ~ $300,000 per day while that of the later is only between $1,000 and $2,000.

[18] http://biz.kbstar.com/quics?asfilecode=5023&_nextPage=page=B005199&boardId=114&bbsMode=view&articleId=8626

Variable Cost of Care

Now, we assume that the cost of care can depend on the number of client security measures. For instance, a user must always unplug the USB digital signage from any public computer he or she had logged on, and must always lock his or her office desk drawer where he keeps key-code cards or one-time-password devices. For simplicity of analysis, we assume the linear function, i.e., *c(x) = cx*. The bank's profit function becomes:

$$\pi_b(x) = \underbrace{\int_{s_1}^{1} f \cdot ds}_{\text{Fee Income}} - \underbrace{\int_{s_2}^{1} p_m s \cdot ds}_{\text{Compensation Expenditure}}$$

With $s_1 = \min\{s_{CB}, s_{LB}\}$ and $s_1 = \max\{s_{CB}, s_{LB}\}$ where $s_{CB} = \frac{f + cx}{p_0 - p_m}$ and $s_{LB} = \frac{kx}{p_m}$.

Unlike the previous fixed cost case, the bank now faces a trade-off. More client security measures yield reduced compensation expenditure for it increases the litigation cost for users, however it also increases cost of care for users. Increased cost of care will cause more users to give up using the service and it will reduce the bank's income from transaction fee. The bank can forfeit income from small transaction users while minimizing compensation expenditure or can take the maximum income from all the potential customers' fee, while fully compensating users' damage from online theft. The profit function of the bank is quadratic and convex over *x*, for $\frac{\partial^2 \pi_b}{\partial x^2} = \frac{k^2}{p_m} > 0$.

Hence, the optimal amount of CSM is always one of boundaries. Then it is obvious that when $x_b^* = 0, \hat{s}_{burden} = 0$ and when $x_b^* = \frac{p_m}{k}, \hat{s}_{burden} = 1$.

In Appendix B, we show that $\pi_b(0) \geq \pi_b(\frac{p_m}{k})$ when $k \leq 2c$ and otherwise, $\pi_b(0) < \pi_b(\frac{p_m}{k})$.

Proposition 3*: Under burden of proof with variable cost, the bank will allocate client security measures at the same level with the fixed cost case when the litigation cost is relatively large and otherwise, it does not allocate any.*

Even with the risk of losing customer because of increased cost of care, the bank will still choose to minimize compensation expenditure by increasing number of client security measures if every additional client security measure creates relatively more litigation cost than the cost of care.

In reality, it may be more likely that the litigation cost is much larger than the cost of care in online transaction. Proving in court that the security devices were perfectly working at the time of the theft would be much difficult than locking the desk drawer containing the security devices. Thus, the bank is more likely to allocate CSM to users.

So far we have only considered short term decisions and both *c* and *k* are given. However, if we consider the long term perspective we may have more intuitional insights. If a bank can invest in technological advancement in a long term, the bank may change both *c* and *k* slightly. However, our model suggests that even with long term investment, bank will not try to reduce *k*, for reducing *k* does not give the bank any benefit. Although the bank may try to reduce *c* to capture more potential customers by long term investment, the fact that the bank has no incentive to reduce *k* can be very problematic to society, since any litigation cost is social dead weight. These intuitional expectations can be a viable answer to "Are banks shifting blame to its users?" for banks alone will not stop assigning litigation cost to its users even with the long term perspective. For example, in regime 2 client security measures given by banks are not equipped with easy-to-use log analysis functions. The logs from each client security measures can be very helpful to users who must fight in court. i.e. reducing litigation costs. However as our model suggests, banks have no incentives to reduce users' litigation costs. We will discuss the government's possible reaction in later sections.

Implications

Optional client side security measures

So far our model only assumed that a bank offers only mandatory sets of client security measures in regime 2. We can easily extend the model with optional client side security measures.

First, a bank can provide "more-than-mandatory" client security measures. While these optional client side security measures do create more cost of care, they do not create any additional burden of proof, for they are not mandatory. Some users will find that with full option, the services are cheaper than basic client security measures which have bigger probability of accidents.

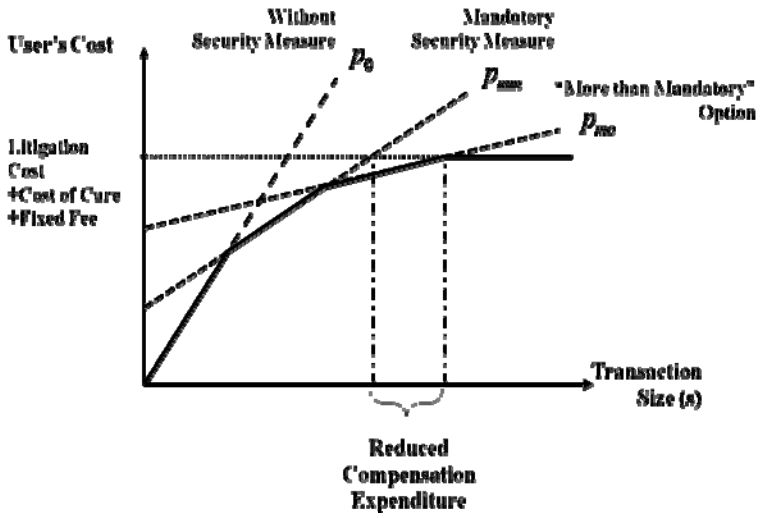

Figure 2. Case of "more than mandatory" option

Figure 2 shows how optional client side security measures affect user's behavior. With full option, the probability of accident will be lower than with only mandatory CSM, $p_{mo} < p_{mm}$. However full options create a higher cost of care, shifting the overall cost curve upward. Some users will find their transaction size is not worth burden of proof, if more optional security measures are available. Therefore, with optional client security measures that exceed mandatory, banks can reduce liability cost further.

On the other hand, banks can provide "less than mandatory" options. The users who only need very small sized transactions will give up using the bank's service because of the excessive cost of care induced from mandatory set of client security measures if no other options are provided. With less than mandatory option, some of those who previously gave up using the service will reconsider if the service provides the better chance of avoiding accident with bearable cost of care. Figure 3 shows the amount of profit from those users who have reconsidered, thus generating more profit for the bank.

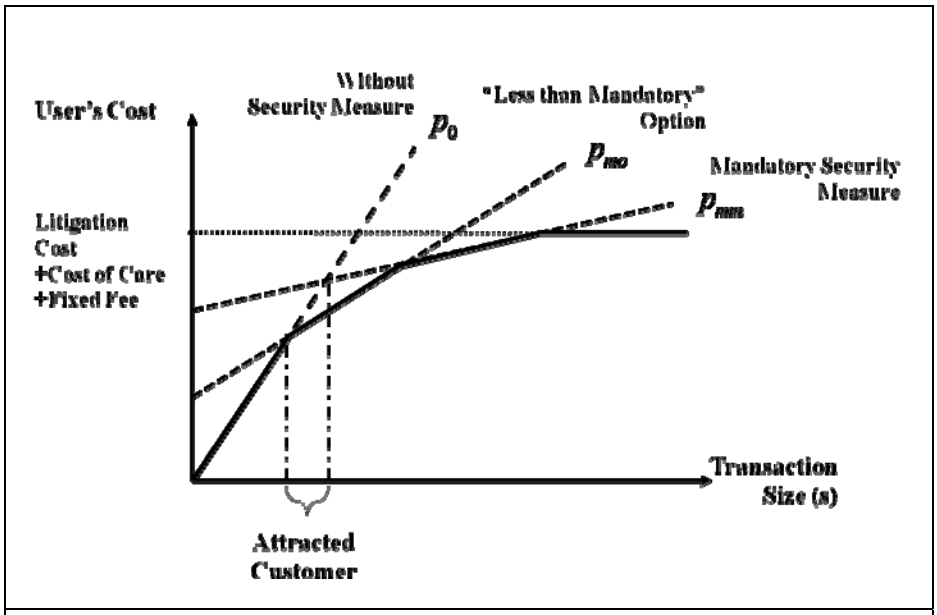

Figure 3. Case of "less than mandatory" option

For each possible option there exists opportunities which can be exploited by bank to attract more customers who couldn't use the bank's service or deter who would definitely sue the bank when only mandatory client side security measures are provided. A bank's manager must investigate their customer's transaction size distribution and decide whether to provide options for potential customers.

We can further extend our implications from optional client security measures to customers across regime. Our bank in regime 1 under strict liability can provide "more than mandatory" client security measures to attract large transaction size users who are willing to bear cost of care for more protection. In earlier sections we have assumed that under strict liability, user is compensated immediately. However in reality compensation still can take some time for days, such inconvenience can sometimes surpass cost of care of security measures. And we can expect the larger transaction size, the more inconvenience from the procedure of being stolen and getting compensation. In this case number of mandatory client security measures is zero. Even with no litigation cost and full compensation, the reduced expected damage is favorable to both users and banks.

On the other hand, banks in regime 2 can provide "less than mandatory" client security measures to attract small transaction size users, who didn't feel the cost of care was too high considering their transaction size. Actually, bank can provide other protection scheme such as insurance, reducing "less than mandatory" number of client security measures to zero. Even with no cyber protection at all, some users will enjoy removed cost of care and bank can capture customers previously unavailable to them. The banks in both regimes have learned from each other, and this "menu of services" is already observable in real world. Further discussions are in the next section.

Menu of services

For bank managers, our findings so far indicate that with a burden of proof (regime 2), a bank can provide client side security measures to its users to maximize its profit. However with too many client side security measures, users with small transaction sizes will stop using the service. It is important that the bank to align its security architecture to its business strategy. If the bank's target customer intends to make transactions large enough to cover burden of proof with online banking, he or she will value security more than the cost of care or burden of proof. Therefore the bank must provide good security measures to capture customers.

In contrast, if the target customer intends to make transactions that are not large enough to cover even the cost of care, the bank must provide various options to reduce the cost of care. Since the target customer is most likely to give up suing if an accident happens, the burden of proof is not important in this case. How to make and how to provide easy-to-use security measures are more important factors.

Under strict liability (regime 1), the bank has a limited number of ways to configure its security architecture, for no one will use client side security measures that induce cost of care. The only method that is actually in use is restriction in transaction size. We can safely assume that a bank's actual cost per electronic transaction is invariant with the transaction size. Therefore additional handling fees for large transaction sizes can be translated as insurance fees. Table 2 shows that banks are charging different handling fees according to transaction sizes and other risk indicators in regime 1. This works exactly as per-transaction insurance, for there is no other way to cover the risk. On the other hand, under burden of proof (regime 2), users are using client security measures intensively. Our model predicts that a bank has a smaller probability of possible accidents, and a smaller expenditure in legal costs in regime 2. Hence, banks in regime 2 will allow very large online transactions, as in Table 1

Table 2. Transaction Size Allowance per Day

Regime 1 (Kookmin Bank) **All online transactions are free of charge		Regime 2 (Citibank)	
Required Client Security Measure	Allowance per day for individual	Destination & Fee	Allowance per day for individual
Keycode Only	Up to $50,000	Between Citibank (Free)	Up to $1,000
Keycode and Cell phone	Up to $250,000	User's account in other U.S. banks (Free)	Up to $2,000
One Time Password	Up to $500,000	Other account in other U.S. banks ($18.75)	Up to $50,000

These legal differences between countries are more important for global firms. If a bank originates from a country which needs burden of proof, the bank must have invested significant amounts of money in client side security measures, which are useless in a country with strict liability. On the other hand, a bank originating from strict liability will have problems in a country with burden of proof, for no user under burden of proof will make use of that service, unless proper security measures are provided to his or her personal computer. From a user's perspective, a user who only needs small size transactions under burden of proof, is annoyed by massive client side security measures and cost of care while a user who needs a large size transaction under strict liability is annoyed by the risky service with high transaction fees.

This brings up the idea about service menu based on self-selection. A bank with well developed client side security measures could sell their services to potential customers who require large transactions under strict liability, while a bank with experience in operating under strict liability could sell their insurance services to potential customers who only need small transactions under burden of proof.

In regime 1, to provide client security measure under strict liability, Let insurance fee $r(s) = r\,s$ is in effect. Then eq. (4) becomes

$$\pi_u = -f - r \cdot s \tag{14}$$

For a more conservative assumption, let c(x) = c x. Then eq. (3) becomes:

$$\pi_u = -f - c \cdot x \tag{15}$$

The users under strict liability will gladly use client security measure, if $r\,s > c\,x$. The bank may provide client security measures if the induced cost of care is small enough, or the required insurance fee for the transaction size is large enough. In regime 1, some banks have recently been selling or providing links for client security measures[19].

Our bank in regime 2 lost customers in case 1, whose transaction size is too small to bear induced cost of care. In order to retain those customers, let our bank provide insurance fees to cover their expected damage. Then the user's expected cost in case 1 changes from:

[19] http://www.usbank.com/cgi_w/cfm/about/online_security/protect_computer.cfm

$$\pi_u = -f - p_0 \cdot s \tag{16}$$

To

$$\pi_u = -f - r \cdot s$$

This is the same as in eq. (16). The users will gladly use a specific bank given that the insurance fee r s is smaller than the expected damage, $p_0 s$ ($r s < p_0 s$).

In regime 2, "Internet Banking Insurance" has been available for banks and service providers since 2007, and restrictions on transaction sizes are in effect and change according to the user's security measures[20]. The banks of both legal schemes are already learning from each other and taking actions to utilize it.

For governments

We have showed in regime 1 which is under strict liability that there can be a prisoner's dilemma working against social welfare, preventing any bank from providing client security measures which can be more beneficial for society. Only strong society-wide external incentives or regulations can break the dilemma and increase social welfare.

Governments, under regime 2, must be aware of differences between client side security measures and server side security measures, for this technological difference affects the outcome of social economic efficiency. Governments must recognize that too many client side security measures are suboptimal, demising welfare of online banking users who only need small transactions. Therefore, governments must set limits on burden of proof by regulating set of mandatory client side security measures. And our findings suggest government agencies should monitor or regulate the effectiveness of client side security measures, for banks do not have enough incentive to maintain effectiveness of client security measures. Banks still can minimize compensation expenditure by throwing more the less effective client security measures to its users. However it is known to be very hard for governments to monitor firm's security effectiveness by government (Anderson, 1994). Moreover, governments must be sure that there are plenty other methods available for small sized transactions. If not, governments may be required to regulate about the easy-of-use in terms of using client side security measures, to maintain the lowest cost of care possible in online banking. In recent report by the Korean Information Security Agency, suggests that the "user-unfriendly nature of online signature system" is bottlenecking online transactions (KISA, 2008). In addition, governments must be aware of long term new technology development opportunities which can reduce litigation cost and impose certain regulations for them, since banks do not have even long term incentives to reduce litigations cost assigned to thier users.

Of course, governments are also responsible of applying appropriate liability in the first place, since it would be very hard to change social-wide liability schemes on the fly. Governments must investigate social-wide online transaction characteristics, like transaction size profiles or the competitiveness of domestic computer security industry. Only a carefully planned liability scheme and specific regulations can overcome an unexpected economical outcome in social welfare.

Conclusions

This paper investigates unique legal effects on online banking security configurations, due to the characteristics of information technology. Under regime 1: strict liability, banks cannot provide adequate client security measures to their users due to incurred cost of care. Although client security measures are needed to lower the probability of accidents to a socially desirable level under server-client architecture, legal costs such as cost of care prevent actual implementation of client security measures. Bank options are limited to transaction size restrictions. Under regime 2: burden of proof, the bank can control its users' cost of care and litigation cost by providing them client side security measures for free. The bank faces a tradeoff between the loss of customers due to enforced cost of care, and the gain in liability costs due to enforced burden of proof. However, if the decision is made by banks, the number of client security measures may be larger than the user's desirable number, or even larger than a socially desirable. This

[20] ebiz@insurance http://post.meritzfire.com/isw/cil/ccn/iccn120k_a1.jsp

affects bank strategies and government responsibilities. A bank should set a fixed number of client side security measures, in other words, the security architecture needs to be aligned with target customer's characteristics. The government should be aware of differences between client side security measures and other security measures to control social costs created by online banking transactions. A global bank may need different security architectures in their services to operate in different liability schemes. A government must consider how bank transactions are executed when it determines its liability scheme.

This paper has limitations and possibilities for further extensions. We have made monopolistic assumptions to describe our arguments. It would be valuable for bank managers if the model can be extended to describe conditions for using cost of care and litigation cost as competitive dimensions for more general strategies. Users' distribution along transaction size has not modeled very realistically, thus extending the model to handle more realistic transaction size distribution can yield richer implications. Financial regulations like Bazel II standard, may have significant effect on our model. Bazel suggest methods for measuring operational risk, which includes theft in online banking. Banks will certainly insist that they need less than the standard mandatory cash reserve, since their client side security measures reduce operational risk significantly. With our model, maybe governments ought to apply litigation costs created by client side security measures, in addition to the proposed amounts of cash reserved by the bank.

Appendix A

We have found that under strict liability, the bank's optimal transaction size is $\hat{s}_{strict} = \frac{f}{p_0}$. In addition, banks must be at least profitable at optimal transaction size. Thus, the following must be held to make any bank operate in regime 1.

$$f\hat{s}_{strict} \geq \frac{1}{2} p_0 (\hat{s}_{strict})^2$$

Which leads to

$$\hat{s}_{strict} \leq 2\frac{f}{p_0}$$

By assumption , $\hat{s}_{strict} \leq 1$. Thus, $2\frac{f}{p_0} \leq 1$. Therefore, $\frac{f}{p_0} \leq \frac{1}{2}$.

Appendix B

We will compare two decisions ($x = 0, x = \frac{p_m}{k}$) by putting each *x* in profit function:

$$\pi_{b,x=0} = \left(1 - \frac{f}{p_0 - p_m}\right) f - \frac{1}{2} p_m \left(1 - \frac{f^2}{(p_0 - p_m)^2}\right) \quad (17)$$

$$\pi_{b,x=\frac{p_m}{k}} = \left(1 - \frac{\frac{c \cdot p_m}{k} + f}{p_0 - p_m}\right) f \quad (18)$$

We want to find the conditions that eq. (15) becomes larger than value of eq. (14)

$$\left(1-\frac{\frac{c\cdot p_m}{k}+f}{p_0-p_m}\right)f>\left(1-\frac{f}{p_0-p_m}\right)f-\frac{1}{2}p_m\left(1-\frac{f^2}{(p_0-p_m)^2}\right)$$

Simplifies to:

$$\frac{1}{2}-\frac{f}{p_0-p_m}\left(\frac{1}{2}\frac{f}{p_0-p_m}+\frac{c}{k}\right)>0$$

Since p0 and pm means expected damage when the largest size transaction has been stolen with no security measures and with security measures respectively, we will assume that transaction fee is relatively small enough to:

$$\frac{f}{p_0-p_m}<\frac{1}{2}$$

Then proposed inequality of our interest holds when:

$$\frac{1}{2}\frac{f}{p_0-p_m}+\frac{c}{k}<1$$

Reduced to:

$$k>2c$$

References

Agre. P. "Introduction in Technology and Privacy: The New Landscape," *The MIT Press*, 1998

Anderson, R.J., "Nine principles," ESORICS, 1994.

Baek, M.Y. "How to improve electronic financial transaction security," *Korea Financial Telecommunications and Clearings Institute*, 2006.

Bank of Korea. "State of Domestic Internet Banking Usage Statistics," *Dept. of electronic finance*, 2009.

Bob Sullivan, "Online bank fraud concerns consumers," *www.msnbc.msn.com/id/6713033/*, MSNBC, 2004.

Caudil. M, Murphy, E. "Consumer Online Privacy: Legal and Ethical Issues," *Journal of Public Policy & Marketing*, Vol.1, 2000

Claessens, J. et al. "On the Security of Today's Online Electronic Banking Systems," *Computers & Security*, vol. 21, 2002.

Comscore, Inc. "comScore State of Online Banking," *Whitepaper*, 2009.

Cooter, Ulen "Law & Economics 4th edition," Pearson 2004, pp. 330-331.

Dorothy Judd v Citibank, 435 NYS, 2d series, pp 210-212, 107 Misc.2d 526.

FFIEC "Authentication in an Internet Banking Environment," *FFIEC Review*, 2005.

Granova, A. et al. "Online banking and identity theft: who carries the risk?" *Computer Fraud & Security*, vol. 11, 2004.

Harrison, Theeuwes "Law & Economics", Norton 2007, pp. 254-257

Identity Theft Resource Center. "Security Breaches 2008," *ITRC Surveys & Studies*, 2009.

Jung. Y.S. "Responsibilities of banks at electronic transactions", Korea Consumer Agency, 2005.

Korea Financial Supervisory Service. "Financial Breaches state report for 5 years," *www.fsc.go.kr*, 2009.

Korea Information Security Agency. "Customer Satisfaction on E-signature," *http://www.kisa.or.kr*, 2008.

Korea Information Security Agency. "State of individual information protection, 2008," *http://www.kisa.or.kr*, 2008

Landes M., Posner R.A., "A Positive Economic Analysis of Products Liability," *Journal of Legal Study*, 1985

Lee, Y.J. "Korean internet securities at emergency", *Business and Computer*, 2005

McCullagh and W. Caelli. "Who goes there? Internet Banking: A Matter of risk and reward", ASISP 2005, Brisbane, 2005

Microsoft. "Online Identity Theft: Changing the Game: Protecting Personal Information on the Internet," 2008

Miller, S.R., Parkhe, A. "Is there a liability of foreignness in global banking? An empirical test of banks' X-efficiency," *Strategic Management Journal*, 2002.

Noam Sher. "New Differences between Negligence and Strict Liability and Their Implications on Medical Malpractice Reform," *Interdisciplinary Law Journal*, Vol. 16, 2007

Peter A. Loscocco, et al. "The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments. In Proceedings of the 21st", *National Information Systems Security Conference*, 1998, pp. 303–314.

Priest, G.L. "The Invention of Enterprise Liability: A Critical History of the Intellectual Foundation of Modern Tort Law," *Journal of Legal Study*, 1985.

Sathye. M. "Adoption of Internet banking by Australian consumers: an empirical investigation," *International Journal of Bank Marketing*, Vol 17, 1999

Shapiro. C. "Information Rules: A Strategic Guide to the Network Economy", *Harvard Business School Press*, Cambridge, 1999

Shumaila Y. et al. "A proposed model of e-trust for electronic banking," *Technovation*, vol. 23, 2003

Singh, S. "The social dimensions of the security of Internet banking," *The social dimensions of the security of Internet banking*, vol. 1, 2006

Siriluck Rotchanakitumnuai, Mark Speece. "Barriers to Internet banking adoption: a qualitative study among corporate customers in Thailand", *International Journal of Bank Marketing*, Vol. 21, 2003

Suh and I.Han, "Effect of trust on customer acceptance of Internet Banking," Electronic *Commerce Research and Applications*, vol. 1, 2002

Wang. Y, et al. "Determinants of user acceptance of Internet banking: an empirical study," *International Journal of Service Industry Management*, Vol. 14, 2003

White H., Nteli F. "Internet banking in the UK: Why are there not more customers?" *Journal of Financial Services Marketing*, Vol. 9, 2004.

Xu, M, Salami B, et al. "How to Protect Personal Information against Keyloggers", *Internet and Multimedia Systems, and Applications*, 2005