[“A” Company Case]

Supreme Court Decision 2013Da43994, 2013Da44003 (consolidated) decided February 12, 2015

Regarding damages arising out of leakage of personal information by “A”company which is not deemed to be in violation of any legal/contractual duty

Judgment of the court below: Seoul High Court Decision 2010Na31510, 31527 (consolidated) decided May 2, 2013

Facts

In order to use the brokerage service for the goods provided by Defendant, “A” company, Plaintiffs provided their name, residents registration number, mobile phone number, and e-mail address to “A” company while they entered into a service use contract and became an online member of Internet open market site of “A” company (the “Site”) under the clause 8 of the said contract.

On around beginning of January 2008, a hacking incident occurred to the “A” company server and, according to the result of police investigation, it was assumed that such hacking incident led to the leakage of membership information of “A” company, which had been stored in the database server, including the name and resident registration numbers of such members five times for the period from around January 4, 2008 to January 8, 2008.

Some persons assumed as Chinese hackers accessed to tomcat server, a web

application installed in enomicx server, one of web servers of “A” company with the ID and passwords in their initial setup on around January 3, 2008; they uploaded a backdoor program named as 'job.war' in the manager page of the said tomcat server; they got into the server for managers; and they found out the ID and encoded passwords of manager for the database server in this case.

Legal issue

How could an ISP be proved to be responsible for damages by failing to take such technological and managerial measures as to ensure the security of personal information?

Summary of Decision

[1] The Information and communications service provider (ISP) shall have the legal duty to take such technological and managerial measures to ensure the security of personal information. Further, when ISP has collected the membership information by means of a mandatory clause of the service contract, ISP also has a contractual obligation to take protective measures necessary for the prevention of loss, theft, leakage, alteration of, or damage to, the personal information of users.

[2] Whether ISP has breached the legal/contractual duty to take necessary safeguards ensuring security of personal information pursuant to Article 28(1) of the former Network Act or the service contract depends on such criteria as

protective measures reasonably expected in a socially accepted sense taking comprehensively into account the standard of universally known security technologies at the time of incident; overall security measures taken by ISP; the development stage of security technology to prevent incidents, etc. In particular, under Article 3-3(2) of the Enforcement Rule of the former Network Act, the technological and managerial measures for personal information protection shall be taken into account. Insofar as ISP has exerted such technological and managerial measures as demanded by the relevant Notifications pursuant to Article 28(1) of the former Network Act, ISP is not deemed to be in violation of any legal/contractual duty to take safeguards except for special circumstances.

Reasoning

The Information and communications service provider (ISP) shall have the legal duty to take such technological and managerial measures as mentioned in the subparagraphs of Article 3-3(1) of the Enforcement Rule (the previous one prior to the MOPAS Decree No. 34 wholly amended September 23, 2008) of the Act on Promotion of Information and Communications Network Utilization and Data Protection, etc. to ensure the security of personal information.

Further, when ISP has collected the membership information by means of an information and communications service contract, whose terms and conditions call for mandatory submission of user's personal information, ISP shall have a contractual duty to take protective measures necessary for the prevention of loss, theft, leakage, alteration of, or damage to, the personal information of users.

Considering the openness of the Internet where the information and communications services are performed and the inherent vulnerability of ISP's networks/operation systems exposed to hackers' infiltration, water-proof security system cannot be realized in view of the speed of technological development and overall social transactional cost. Any security technology is essentially a posteriori countermeasure against hackers' attack. Therefore, whether ISP has breached the legal/contractual duty to take necessary safeguards ensuring security of personal information pursuant to Article 28(1) of the former Act on Promotion of Information and Communications Network Utilization and Data Protection, etc.(the previous one prior to the Act No. 8852 amended February 29, 2008, hereinafter referred to as the "former Network Act") or the information and communications service contract depends on such criteria as protective measures reasonably expected in a socially accepted sense taking comprehensively into account the followings: the standard of universally known security technologies at the time of incident; the line and size of business of ISP; overall security measures taken by ISP; cost and benefit accompanied by such security measures; the level of hacking technologies; the development stage of security technology to prevent incidents, contents of personal information collected by ISP, the scope of damages caused by data leakage to users, and so forth.

Under Article 3-3(2) of the Enforcement Rule of the former Network Act, the Minister of Information and Communication shall set forth and make a notification of specific standards for protective measures subject to each

subparagraph of paragraph (1) and, accordingly, the technological and managerial measures for personal information protection (Ministry of Information and Communication Notification No. 2005-18 and No. 2007-3, hereinafter referred to as the "Notifications") prepared by the Minister of Information and Communication shall be taken into account.

Insofar as ISP has exerted such technological and managerial measures as demanded by the relevant Notifications pursuant to Article 28(1) of the former Network Act, ISP is not deemed to be in violation of any legal/contractual duty to take safeguards except for special circumstances.

In addition, it is also hard for this Court to jump to the conclusion that "A" company failed to prevent such hacking incident by not taking necessary protective measures to ensure the security of personal information.

As alleged by "A" company, considering relevant legal principles and records regarding the grounds for appeal, this Court rules that the decision of the lower court was reasonable and, there is no unlawful act of misunderstanding in construction of such Notifications and on legal principles in terms of damage responsibilities of ISP as alleged as ground for appeal.

Conclusion

Therefore, all appeals are dismissed, and the costs of the appeal are assessed against the losing party. It is so decided as per Disposition by the assent of all participating Justices.