The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 16, No. 2, pp.1-8, Apr. 30, 2016. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2016.16.2.1
JIIBC 2016-2-1

간편결제 서비스에서 전자금융사고 시 국내 사이버 배상책임보험의 한계 및 개선방안에 대한 연구

A Study on Improving Cyber Liability Insurance for Electronic Financial Incident in Easy Payment System

이한준*, 김인석**

Han-Jun Lee*, In-Seok Kim**

요 약 정보통신기술의 발달 및 인터넷 이용의 활성화로 간편결제 등 금융과 정보통신기술의 융합된 핀테크 산업이 활성화 되고 있다. 하지만 현재 법규 상 금융사고 발생 시 금융회사, 핀테크 업체와 소비자 간의 책임이 모호하고 금융기관 또는 전자금융업자가 손해배상을 해야 하는 경우 전자금융거래법 제정('06년) 당시 지정된 전자금융사고 책임이행 보험 가입 최저한도와 현재 전자금융거래 규모, 사고 발생 추이, 보안 투자 규모 등을 비교했을 때 현실적으로 적정하다고 보기 어렵다. 이에 본 논문에서는 국내 금융사고의 현황과 사후처리를 파악하고 현재 사이버 배상책임보험의 한계와 변경 필요성을 지적하고자 한다.

Abstract A convergence of finance and information technology brought a remarkable development in Fin-Tech industry. On the other hand, currently existing laws seemed inappropriate to address the liability of financial institutions, Fin-tech enterprises and consumers in case of financial accidents due to its ambiguity. The minimum insurance obligation by financial institutions specified under the Electronic Financial Transaction Act 2006 is not keeping with current reality, considering transaction volume, frequency of incidents, and security investments. This paper aims to lay stress on the need of cyber liability insurance by understanding the domestic financial incidents and management, and the limit of existing insurance policy.

Key Words : easy payment system, fintech, Cyber Liability Insurance

Ⅰ. 서론

정보통신기술의 발달 및 인터넷 이용의 활성화로 사업자들이 수많은 개인정보를 수집하고 이용함으로 고의 또는 과실에 대한 개인 정보를 제3자에게 유출하거나 제3자가 해킹 등의 불법적인 방법으로 개인정보를 빼가는 사례가 늘고 있으며, 그 피해규모 또한 갈수록 커지고 있다. 2014년 Allianz Risk Barometer survey 에 따르면 글로벌 비지니스 리스크 Top 10에 사이버 범죄, IT 시스템 고장 등에 의해 발생하는 사이버 상의 손해가 전체 경영 리스크의 12%를 차지하며 새로운 리스크로 부상했다. 2013년에 정보보호 유출 사고 건수와 유출된 정보의 수는 각각 619건과 8,790만 건으로서 2012년도에 비해 38%, 40% 증가하였다. 정보 유출의 평균비용은 188달러로 집계되지만 다양한 피해 대상과 경로를 통해 유출되었고 눈에 보이지 않는 손실이 대부분이므로 정확한 피해액을

*준회원, 고려대학교 금융보안학과
**정회원, 고려대학교 사이버국방학과(교신저자)
접수일자 : 2016년 3월 5일, 수정완료 : 2016년 4월 5일
게재확정일자 : 2016년 4월 8일

Received: 5 March, 2016 / Revised: 5 April, 2016 / Accepted: 8 April, 2016
**Corresponding Author: iskim11@korea.ac.kr
Dept. of Information Security, Korea University, korea

파악하는 것이 힘들다. 그렇기 때문에 불법적인 정보 유출을 예방하고자 개인정보보호법, 신용정보의 이용 및 보호에 관한 법률, 정보통신망 이용 촉진 및 정보보호 등에 관한 법률에 소송제도, 징벌적 손해배상제도 등 각종 예방조치들을 규정하고 있다.

간편결제 서비스 등 핀테크 산업이 활성화 되면서 전자금융 사고 시 금융회사와 플랫폼을 제공해준 IT업체 사이의 책임문제가 대두되고 있다. 또한 자본여력이 크지 않은 IT업체가 피해자에게 배상할 경제적 능력이 없을 경우 실질적으로 피해자들이 충분한 구제를 받을 수 없게 되는 문제가 발생하게 된다. 전자금융거래법 제정('06년) 당시 전자금융사고 책임이행 보험 가입 최저한도를 지정하였지만 제정 당시와 현재 전자금융거래 규모, 사고 발생 추이, 보안 투자 규모 등이 달라졌기 때문에 현실적으로 적정하다고 보기 어렵다. 본 연구에서는 국내 금융사고의 현황과 사후처리를 파악하고 현재 사이버 배상책임보험의 문제점을 지적하고자 한다.

II. 관련 연구

1. 간편결제 서비스의 정의

간편결제 서비스란 모바일 거래를 포함한 온라인 상거래 구매자가 신용카드 정보, 계좌정보 등의 결제정보를 최초 1회 또는 최소한의 횟수로 입력하고 결제 시에는 비밀번호 등의 인증만으로 결제를 완료하는 방식의 서비스를 통칭한다.[1]

2. 간편결제 시장

글로벌 간편결제 시장은 모바일 기기의 보급 확산과 O2O(Online-to-Offline) 시장의 성장, 최근 급속히 확산되고 있는 핀테크 산업의 성장과 연계되어 고성장 추세에 진입하고 있다. 특히나 글로벌 고객을 통화나 결제시스템에 구애 받지 않는 지급결제 서비스를 제공한다는 점에서 앞으로도 지속적인 성장을 할 것으로 예상된다.

Gartner의 자료에 따르면 글로벌 모바일 결제시장 규모는 2011년 1,000억 달러 내외에서 2017년에는 7,200억 달러 규모로 성장할 것으로 예상되며, 결제 건수도 2012년 110억 건 수준에서 2015년에는 470억건 수준으로 급성장할 것으로 보고 있다. 또한 온라인 상품시장이 2016년에는 1,8조 달러로 성장할 것으로 전망되며 그 중 모바일 상품시장의 규모가 6,160억 달러로 성장할 것으로 예상되고 있다.

국내 시장도 글로벌 시장의 패턴과 유사한 형태로 진행되고 있는 것으로 파악되고 있다. 국내 온라인쇼핑시장은 2010년 27조원 규모에서 2014년에는 45조원 규모로 성장하면서 연평균 18.1% 성장하였다. 반면 모바일쇼핑 시장은 2010년 3천억 원 규모에서 2014년 13.2조원 규모로 연평균 157%의 빠른 성장세를 기록하였다. 2014년 소셜커머스 상품의 60%가 모바일을 통해 판매된 것으로 나타났고, 이는 향후 모바일 상품 시장의 성장이 더욱 가속화 될 것으로 전망할 수 있다.[2]

3. 국내 전자금융사고 대응 현황

가. 사전적 대응

감독당국과 업계에서는 전자금융사고가 가장 빈번하게 발생하는 클라이언트 구간, 데이터 전송을 하는 네트워크 구간과 해당 데이터가 저장, 활용되는 시스템 구간으로 나누어 사전적 대응을 하고 있다. 클라이언트 구간 보안대책으로 사용자 인증 강화, 사용자 접근매체에 대한 해킹, 사기 방지 툴의 보안 및 개선, 사용자 보안의식 고취가 있다. 네트워크 구간에서의 보안대책은 2가지 원칙을 필요로 한다. 하나는 정당한 사용자의 접속을 판별하는 것이고 다른 하나는 접속 이루 송수신 데이터에 대한 기밀성이 보장되어야 한다는 것이다. 이를 위하여 물리적 안정성 확보를 위한 전용선 도입 또는 주민등록번호, 계좌번호, 계좌 비밀번호 등의 송수신 데이터에 대한 암호화를 적용하고 있다.[3] 감독당국은 전자금융 감독규정에 근거하여 금융기관 및 전자금융업자 등에 대한 시스템 보안대책을 제시하고 있다.[4] 정보처리시스템 및 전자금융업무 개발 및 운영 담당 인력과 조직을 통제하는 인력의 운용에 관한 사항, 각종 재해 등 내 · 외부 충격으로부터 전산실을 보호하고 업무연속성을 확보할 수 있는 공간적 개념의 시설 보호에 관한 사항, 정보 처리시스템 접근 단말기, 전산자료, 정보처리시스템과 같은 전자적 장치의 보호에 관한 사항을 정함으로써 시스템 안전성 확보를 유도하고 있다.

나. 사후적 대응

현행 전자금융거래법 제9조 제1항에 따르면 접근매체의 위조나 변조로 발생한 사고, 계약체결 또는 거래지시의 전자적 전송이나 처리과정에서 발생한 사고로 인해

표 1. 전자금융사고 대비 보험 공제 가입기준
Table 1. Domestic Standard of Compensation Insurance Against Electronic Financial Incidents

구분		보험금액	대상기관
금융 기관별	은행권역	20억 원	시중은행, 농협중앙회, 기업은행, 농협 단위조합(공동가입)
		10억 원	지방은행, 외은지점, 수협중앙회, 산업은행, 체신관서, 신용카드업자, 수협 단위조합·신용협동조합·상호저축은행·새마을금고(공동가입)
	증권권역	5억 원	증권회사, 증권금융, 선물업자
	기타	1억 원	전자금융거래법 및 시행령상 금융기관 중 위 금융기관을 제외한 금융기관 (예) 보험회사, 상호저축은행(공동보험 가자 제외), 여신전문금융업자(신용카드업자 제외) 등
전자금융 업무별		2억 원	전자자금이체업, 직불전자지급수단 발행업
		1억 원	전자화폐 발행업, 선불전자지급수단 발행업, 지급결제대행업, 결제대금예치업, 전자고지결제업 등

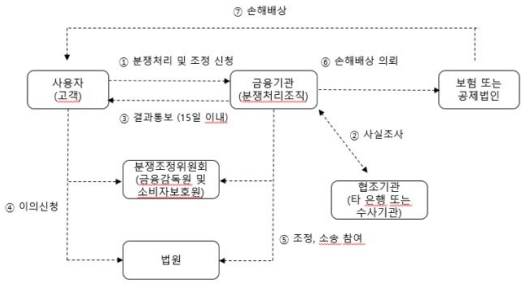

그림 1. 전자금융 분쟁처리 절차
Fig. 1. Dispute Settlement Procedures in Electronic Financial Transactions

사용자에게 손해가 발생한 경우 원칙적으로 금융기관 또는 전자금융업자가 손해 배상책임을 갖는다. 아울러 동법 제27조에서는 전자금융거래와 관련한 분쟁처리 및 분쟁조정 절차를 마련토록 규정하고 있는 바, 금융기관 또는 전자금융업자는 그림 1과 같은 일반적인 분쟁처리 및 조정절차를 정하고 있다. 분쟁처리 결과 금융기관 또는 전자금융업자가 손해배상을 해야 하는 경우, 이들은 보험·공제 또는 적립된 준비금으로 사용자에게 보상을 하게 된다. 이 같은 배상책임 이행을 위해 전자금융거래법은 보험·공제 가입 또는 준비금 적립을 의무화하고 최소 금액 기준을 표 1과 같이 정하고 있다. 전자금융사고 대비를 위한 주요 보험 상품으로는 전자금융거래 배상책임보험, 개인정보유출 배상책임보험, e-biz 배상책임보험 등이 대표적이다.

Ⅲ. 국내 사이버배상책임보험의 현황

1. 사이버배상책임보험의 정의

사이버 배상책임보험은 e-business, 인터넷 네트워크 및 정보 자산 등 사이버 리스크와 관련하여 계약자와 제3자의 리스크를 담보하는 보험으로 보험에 가입된 금융사들은 정보유출로 인한 피해와 사기 등 금융 사고를 입었을 때 피해를 입은 소비자에게 먼저 보상해주고 보험사로부터 손실액을 보전 받는다. 보험사는 향후 금융사고에 대한 책임소재를 따져 책임 있는 기업, 혹은 개인에게 구상권을 청구하는 구조다.

2. 국내 사이버배상책임보험 현황

국내에는 개인정보 유출 관련 전자금융거래 배상책임보험, 공인전자문서 보관소 배상책임보험, 집적정보통신시설 사업자 배상책임보험, 개인정보 유출 배상책임 보험, e-biz 배상책임보험 등이 있으며 시장 규모는 연간 241억 원 정도로 추산된다. 하지만 국내 사이버 배상책임보험은 대부분 의무보험으로 전체 산업에서 차지하는 수준은 미미한 상황이다. 실제로 2010년 기준 사이버 배상책임보험 보험료는 78억 원으로 손해보험 전체 보험료 51조원의 0.015% 수준에 불과하다. (표 3[5])

Ⅳ. 해외 사이버배상책임보험의 현황

해외에서 일어나는 전자금융사고가 우리나라 은행권에서 벌어지는 금융사고 빈도수보다 높음에도 선 보상, 후 조사 구조를 가질 수 있었던 것은 사이버 배상책임보험을 가입했기 때문이다. 또한 보험사로선 보험액 지급의 투명성과 사기로 인한 피해를 막기 위해 고객인 금융사의 사이버 리스크를 줄이는데 초점을 맞춘다. 무엇보다 보험사들은 피해금액을 지급하기 전에 미리 사기행위

표 2. 금융회사 개인정보 유출 배상책임보험 가입현황
Table 2. private information liability insurance status by financial company

Classification	Survey	Join	Non-participation
Bank	17	9	8
Life insurance	25	12	13
Loss insurance	15	15	0
Credit company	58	4	4
Stock company	13	13	0
Total	78	53	25

나 금융 사고를 방지하기 위해 FDS를 진화시켜 왔다. 결과적으로 금융 시스템 전체가 사기와 같은 금융사고에 선제적으로 대응할 수 있도록 선순환 구조가 만들어진다.

1. 미국

미국의 사이버 보험시장은 2003년 개인정보 유출 고지 법(Data Breach Notification Law)을 도입한 이후부터 보험시장의 급속한 성장을 했으며, 특히 개인정보 유출 고지 법 내 사업자들의 정보유출시 통지 의무조항으로 인해 법 시행 이후 개인정보유출사고 통계가 급격히 증가하였다. 사이버 보험 상품에 대한 높은 수요(그림 2[6])에도 불구하고 보상 기준 및 규모와 관련해서는 논란이 있는 상황이며, 언론매체 뉴욕 타임즈(New York Times)는 해킹 피해가 대부분 무형적인 형태로 나타나기 때문에 손실을 정량화하기가 쉽지 않다고 설명하고 있다. 또한, 대부분의 데이터 유출사고가 주목받지 못하거나 기업 이미지 차원에서 공개되지 않기 때문에, 보험 업체들이 보상액 산정을 위한 기초 데이터 수집에 어려움을 겪고 있다. 현재 정보보호 보험의 구체적인 보상 내용은 보험회사에 따라 각기 다르지만, 일반적으로 표 4와 같은 내용이 정보보호 보험의 보상범위가 되고 있다. 이외에도 피해기업이 해커 등으로부터 협박을 받았을 경우 합의를 위해 필요한 합의금 등 기업들이 사이버 공격을 받으면서 발생하는 다양한 상황에 대한 보상을 마련하고 있다.

2. 영국

2015년 3월 영국보험자협회 (Association of British Insurers)와 Lloyd 조합이 사이버보험 개발 가이드라인을 제정하면서 영국의 사이버배상책임 보험이 활성화되었다. 영국 정부 또한 사이버보험을 활성화함을 표명하고 그 일환으로 보험사의 사이버보안 사고 분석 능력을

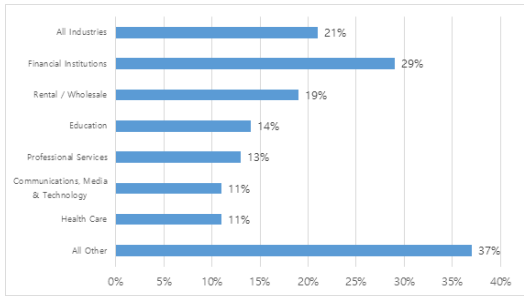

그림 2. 미국 회사들의 사이버책임배상보험 구매 증가율
Fig. 2. Increase in Purchase of Cyber Insurance Among U.S. Companies, 2013

표 3. 정보보호 보험 대상
Table 3. Security information insurance

Range	Contents
Loss of data or damage	Privacy and data leakage damaged by cyber attacks such as viruses, malware, trojans and so on in corporate
Business interruption	Costs for investigating and damaged business operations caused by cyber attacks
Promotion activity	Promotion costs for improving images of corporate damaged by cyber attacks
Liability	Costs incurred for being cited liability about leakage of personal information, infringement of intellectual property in lawsuit

표 4. 영국 전체 가입보험상품 중 CLI 비중
Table 4. CLI proportion of UK insurance
***() : the criteria of 2014**

	Security insurance rate of UK in 2015	CLI proportion of insurance products
Major Company	39% (52%)	2%
S.M.E	27% (35%)	0%

제고를 위한 사이버보안 인증시스템 (Cyber Essentials System) 을 참조하여 대기업을 포함한 중소기업의 사이버보안 사고에 대한 분석을 실시하도록 권고하였다.[7] 그 후 영국정부와 영국의 주요 보험회사이자 위험관리회사인 Marsh 보험회사는 사이버보험의 위험관리 역할 (UK cyber security: the role of insurance in managing and mitigating the risk) 보고서를 발간하여 스트레스 테스트(그림 3[8]) 등을 이용하여 사이버공격의 위험도 수치화 방법을 제시하는 등 사이버 보험 상품을 개발하고 이를 기업의 사이버보안 측정도구로 활용할 수 있는 공동 계획을 발표하였다.

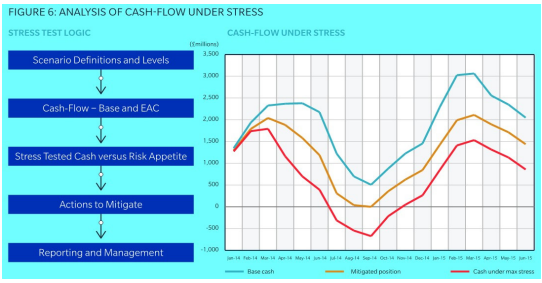

그림 3. 스트레스 테스트 분석 예시
Fig. 3. Analysis of cash flow under stress

Marsh는 금융사의 사이버 보험 가입절차로 기업의 위험관리에 대한 조언뿐만 아니라 발생 가능한 사이버 리스크를 해당 회사의 사업 모델과 비교하여 맵핑(Risk Mapping)하고 세부적인 위협 시나리오를 도출하는 서비스를 추가로 제공하고 있다. 이러한 서비스를 토대로 Marsh는 위험을 산정하여 기업에 알맞은 보험 상품과 적용범위를 알려주는 맞춤형 사이버보험 상품을 제공하고 있다.

3. 일본

일본 CLI시장의 규모를 보면 2012년 AIG가 출시한 Cyber Edge Premium 상품이 76억 엔의 수익을 올렸고 2015년 Tokyo Marine 이 출시한 Cyber insurance Premium 상품은 106억 엔의 수익을 올리는 등 현재 CLI에 대한 관심이 높다. 그 중 개인정보유출에 대비한 보험은 대형 IT업체를 대상으로 한 상품과 중소기업을 대상으로 한 단체보험이 판매되고 있으며 단체보험의 경우 개인정보유출보험이란 명칭으로 일본상공회의소 및 지방상공회의소의 회원을 대상으로 판매되고 있다. 이 상품은 배상책임 부분과 비용손해 부분으로 구성되며 피보험자에게 보험기간 중 일본 국내에서 손해배상 청구가 이루어진 경우에만 보상하고 있다. 신용카드번호, 계좌번호 또는 비밀번호 등의 유출로 인한 손해는 신용카드 번호 등 유출위험 담보 특약을 계약한 경우에만 보상한다. 또한 단체할인 보험료를 적용하며 개인정보보호법에 대응한 리스크진단 서비스를 무료로 제공하여 중소기업의 개인정보유출리스크를 줄이는데 기여하고 있다.[9]

표 5. 일본 개인정보유출보험 보험료 수준
Table 5. Personal information leakage insurance premium levels

Classification (Annual revenue : million yen)	Liability limit by compensation	Liability limit by cost	Premium
20,000 convenience store	300 million yen	30 million yen	about 600,000 yen
10,000 Internet retailers etc.	100 million yen	30 million yen	about 500,000 yen
3,000 Information service providers etc.	50 million yen	10 million yen	about 300,000 yen

V. 국내 사이버배상책임보험 한계와 개선방안

1. 국내와 해외 사이버배상책임보험 비교

국내와 해외 CLI의 차이는 담보 차이에서 발생한다. 국내 사이버 위험과 사이버 보험에 관한 연구를 살펴보면 미국의 CLI는 손해배상금 및 소송관련 비용을 기본으로 컴퓨터 관련 직접적인 손해에 대해 외주업체 직원 제3자의 과실, 고의적인 유출 등 20개의 다양한 담보를 제공하고 있다. 일본의 경우도 해킹, 바이러스 관련 손해배상 비용, 사이버 범죄 유죄 판결 시의 위자료 비용 등 19개의 담보 내용을 포함하고 있다. 하지만 국내 CLI는 데이터 재건과 대체 비용, 개인정보 유출로 인한 손해배상 비용, 네트워크 안전 확보 실패로 인한 손해배상 비용, 도난당한 정보가 공적으로 노출되었을 때 손해배상 비용, 해킹 및 바이러스 관련 손해배상 비용, 사이버 범죄 유죄 판결 시의 위자료 비용, 기술적인 오류나 부주의로 인한 손해배상 비용 등 총 7가지 항목에 대해서만 담보로 제공하고 있다.(표 7[10]) 이러한 차이는 국가마다 제도 차이로 볼 수 있다. 미국의 47개 주는 민간 또는 정부 기업이 개인정보유출이 되면 개인에게 통지해야 하는 법을 제정해 연방정부가 은행, 신용조합, 보험, 건강정보 등을 취급하는 산업에 대해 개인정보유출통지를 요구하고 있다. 유럽의 경우 국가마다 다른 법이 시행되고 있지만 대략 2016년에는 유럽연합 정보보호법에 의해 일원화될 예정이다. 아시아 또한 일관된 법을 시행하고 있지는 않고 인도 등 일부 국가에서는 정보보호법이 존재하지 않는다.

표 6. 한국과 미국의 CLI 비교
Table 6. CLI comparison between korea and USA

<table>
<tr><td>Classification</td><td colspan="3">Domestic liability insurance related to private information</td><td colspan="2">CLI in USA</td></tr>
<tr><td>Object</td><td colspan="3">• Contractors dealing with customer information and industry such as financial institutions and e-financiers, certified electronic document storage, online shopping and Internet development industry etc.</td><td colspan="2">• Various companies such as financing, manufacturing, communications, technology industry which may cause direct damage to a computer-related</td></tr>
<tr><td rowspan="3">Covered damages</td><td rowspan="2">Personal Information extrusion</td><td>Basic warrant</td><td>• Legal costs for third party protection</td><td colspan="2" rowspan="3">• Legal costs for infringement of privacy security
• Costs related to privacy infringement such as information disclosure notification and credit monitoring
• Costs related to corporate assets electronically stored and updating, replacement
• Costs related to privacy infringement about business interruption and security
• Liability costs for reputation damages such as defamatory, infringing throught out printed media or websites, social media
• Costs related to cyber terrorism
• Compliance costs related to billing errors, emergency medical treatment
• Liability costs for information leakage, negligence, negligence, willful damage of third paryt or internal staff as well as hacking, viruses, cyber attacks
• Rreputation recovery costs etc</td></tr>
<tr><td>Optional warrant</td><td>• Risk management costs by the risk management consulting firm
• Costs for protecting the leakage of personal information by the insured
• Third-party economic damages caused by information leaks etc</td></tr>
<tr><td>e-biz</td><td colspan="2">• Liability costs for protecting damages of third party caused by cyber risk such as internet and network activities</td></tr>
<tr><td rowspan="2">Don't cover damages</td><td>Personal Information extrusion</td><td colspan="2">• Claims for damages caused by the criminal actions or intentional of the insured's officers
• Claims for damages caused by information leaks</td><td rowspan="2">Service</td><td rowspan="2">• Services for recovering isssues about security and information infringement</td></tr>
<tr><td>e-biz</td><td colspan="2">• Claims for damages due to intentional
• Claims for damages due to spread non-prevented virus</td></tr>
</table>

현재 정도의 차이는 정보의 종류와 산업의 차이가 있지만 프랑스, 독일, 영국, 일본, 중국은 개인정보유출통지에 대한 의무가 존재한다. 우리나라의 경우도 2011년 9월부터 개인정보보호법을 시행하여 개인정보유출사실 통지를 의무화하였다. 그래서 국내 개인정보 유출관련 보험을 살펴보면 제 3자 보호를 위한 손해배상을 주 담보로 제공함을 알 수 있다.

2. 국내 사이버배상책임보험 한계

해외 시장과 비교했을 때 국내 사이버배상책임보험이 차지하는 시장이 낮은 이유는 낮은 시장성 들 수 있다. 약관에 다양한 면책사유 포함, 법원의 친기업적 판결로 인한 손해 발생사례 부족, 낮은 위자료 판결 액수, 그리고 담보하는 리스크의 다양성 부족이 사이버배상책임보험의 시장을 저해하는 요소로 꼽히고 있다.[11] 또한 미국, 영국, 일본 등의 해외 국가들은 의무보험에 가입을 강제화 하고 있지 않지만 국내의 경우 의무보험 가입을 강제화하고 있다. 이렇기 때문에 대부분의 금융기관 또는 전자금융업자가 법에서 정해진 최소한의 보험에 가입하고 있어 사고 발생 시 법적인 문제를 회피할 수 있다는 점도 간과할 수 없다.

국내 사이버배상책임보험의 다른 한계점으로 책임소재에 대한 명확한 구분이 아직 되어 있지 않다는 점이다. 지금까지 결제수단 및 시스템의 하자, 공인인증서의 결정적인 흠결로 인한 전자금융 사고는 거의 없었기 때문에 전자금융거래 배상책임보험의 역할도 금융회사의 과실인지 고객의 과실인지 결정하는 것이 중요 사항이었다. 하지만 간편결제 서비스에는 고객의 부주의 보다는 채택된 시스템에 대한 기술적인 하자를 가려내야하기 때문에 기존 전자금융거래 배상책임보험 체계만으로는 다소 미

흡하다. 또한 기존 공인인증서 결함 시 향후 구상권 청구가 가능한 공신력 있는 주관 기관이 존재하나 간편결제의 경우 중소규모 업체들이기 때문에 배상 능력에 의문이 생긴다. 게다가 핀테크 간편결제 수단의 경우, 도입초기라 현실적으로 손해보험업계에서 적정한 보험료율 산정이 쉽지 않다는 문제점도 있다. 리스크를 반영해 최초 보험료가 높게 책정될 경우 금융회사의 부담이 높아질 수 있고, 간편결제 활성화에 저해 요소로 작용될 우려가 있다는 점도 지적되고 있다.

3. 국내 사이버배상책임보험 개선방안

가. 사이버배상책임보험의 적정 금액 산정

현재 사고피해 보상보험은 전자금융거래법이 제정 시 도입한 것으로 보험가입 최저한도를 변경 없이 유지해 온 것이다. 하지만 현재 거래 규모와 전자 금융사고 발생 수와 위험도 등 고려했을 때 현실을 적절히 반영하지 못하고 있다. 또한 핀테크 활성화, 규제 완화, 전자 금융업자의 영세성 등을 감안했을 때 현재의 보험가입 최저한도를 높이는 것은 여러 가지 상황을 고려해야 한다. 지금까지 전자금융 사고 발생 시 피해 보상 현황을 살펴보면 은행 등 금융회사는 보험 가입과 관계없이 충분한 보상 여력이 있지만 전자금융 사고 위험도가 높은 규모가 영세한 전자지불중계업자나 간편결제 서비스 제공자들에게 과도한 보험 가입과 금액은 새로운 서비스의 진입을 막을 수 있다. 그렇기 때문에 거래 규모, 이용자 수, 이용수단, 위험 노출 강도, 자본금, 이익규모 등을 고려해 추가적인 피해에 대비한 보험은 기업의 규모에 따라 보상한도를 정하여 보험 상품을 개발하고 금융 회사나 전자금융업자들은 본인의 규모에 적합한 보험을 자율적으로 가입하는 것이 필요하다고 본다. 사고나 장애가 많은 기관은 더 많은 보험에 가입할 것이고 정보보호나 시스템의 안전성이 높은 기관은 적은 보험에 가입할 것이다. 기업 규모에 맞는 사이버 배상책임보험의 도입은 시스템에 대한 투자와 보험 의존도 간의 균형을 맞출 것이다.

현재 은행권에선 전자금융거래사고에 대비해 전자금융거래 배상책임보험을 활용하고 있다는 점, 전자금융사고 발생 시 이용자의 과실 부문을 제외하고 보험금을 지급할 수 있다는 점, 보험율 산정은 매년마다 사고발생 성격과 추이를 감안, 손해사정인의 산정작업을 통해 반영한다는 점에서 핀테크 시대에 금융사고 사후 대응책으로 사이버배상책임보험을 활성화시키는 것이 현실적인 대안으로 고려되고 있다. 하지만 위에 언급했듯 기존의 사이버배상책임보험은 한계점이 있기에 몇 가지 부분에 있어서 변경이 필요하다. 현실의 전자금융 거래규모나 위험도를 반영해 배상책임보험 가입금액을 상향으로 조정하는 방법도 있겠지만 이는 소형 금융회사나 간편결제 서비스 제공자에 대한 부담으로 작용할 수 있기에 바람직하지 않다고 판단된다.

국내보다 간편결제 서비스가 먼저 적용된 미국, 영국, 일본 등 여러 해외 국가들의 경우 국내와 달리 금융회사 및 전자금융업자들에게 의무보험 가입을 강제화하고 있지 않다. 그럼에도 개별적으로 충분한 보험에 가입되어 있음을 확인할 수 있었다. 따라서 법이나 규정에서 보험 가입에 대한 가이드라인을 없애는 것도 하나의 방법이 될 수 있겠지만 기존의 제도를 없애는 것보다 법에서 정한 전자금융거래 배상책임보험이외에 정보유출사고, 시스템 마비 등 피해에 따른 다양한 보험 제도를 마련하고 추가 가입하도록 권고하여 영세 전자금융업자나 간편결제 서비스 제공자에게 부담을 없애고 대형사고 위험이 높은 금융회사들에 대한 피해보상을 확보할 수 있도록 운영하는 것이 바람직하다고 판단된다.

앞으로 비대면 인증의 허용과 인터넷 전문은행의 도입 등은 간편결제 서비스 시장에 큰 영향을 미칠 것이다, 또한 정보보호시스템이 발달되는 만큼 새롭고 다양한 공격 패턴이 등장할 것이다. 그렇기에 전자금융사고 발생 시 대응방안은 꾸준히 논의가 되어야 하며 시대에 맞게 개선되어져야 한다.

Ⅵ. 결론

본 논문에서는 간편결제 서비스와 전자금융사고 발생 시 현재 대응방법을 살펴보고 국내외 사이버배상책임보험을 비교하여 개선방안을 제시하였다.

References

[1] Hyun Ah Jo, “Trends of easy payment services on national and international non-financial institutions,” Payment and Information Technology No.58, pp. 4, Oct. 2014

[2] Cheol Young Kim, "Easy payment market", Hyundai able Daily, July. 2015.
[3] So Yee Kim, "Status and types of Electronic Banking incidents", Payment and Information Technology, Oct, 2009
[4] The commentary of Regulation on Supervision of Electronic Financial Activities, Financial Supervisory Service
[5] "Payment status of Personal Information Disclosure Liability Insurance by financial companies", Financial Supervisory Service
[6] "Benchmarking Trends : Interest in Cyber Insurance Continuis to Climb, March Risk Management Research Briefing", April, 2014\
[7] So Yang Lee, "A plan and prospect of UK Cyber insurances", KIRI Weekly Issue, May, 2015
[8] "UK cyber security: the role of insurance in managing and mitigating the risk", HM Government, March, 2015
[9] Korea Insuranca Development Institute, "The Activation measures on personal information disclosure liability insurance", CEO REPORT, Dec, 2012
[10] Byeon Hwan Bae, Gyeong Sik Min, "Policy Proposals on Activation measures of domestic insurance market", Internet & Security Focus, July, 2013
[11] So Yeon Kim, "A study on domestic cyber danger and cyber insurance", Korean Insurance Academic Society, 2014

저자 소개

이 한 준(준회원)

• 2015년 3월~현재 : 고려대학교 정보보호대학원 금융보안학과 석사과정

김 인 석(정회원)

• 2008년 : 고려대학교 정보경영공학과 (박사)
• 2009년~현재 : 고려대학교 정보보호대학원 교수
• 現 FDS산업포럼 회장, 한국사이버정보전학회 운영위원 등

※ 본 연구는 미래창조과학부 및 한국인터넷진흥원의 "2016년 고용계약형 정보보호 석사과정 지원사업"의 연구결과로 수행되었음