http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.22, No.4, November 2017, pp.21-38
https://doi.org/10.7838/jsebs.2017.22.4.021

개인정보의 제3자 제공시 정보보호 관련 법상 책임에 관한 연구/OPEN API 이용 핀테크 기업을 중심으로

A Study on the Liability of Information Protection for the Third Party Supply of Personal Information/Focus on Fintech Companies Using OPEN APIs

김조은(Jo-eun Kim)*, 김인석(In-seok Kim)**

초 록

금융회사, 공공기관 등이 보유하고 있는 다양한 정보를 오픈 플랫폼을 통해 적극적으로 핀테크 기업에게 개방하고 있는 추세다. 본 연구에서는 개인정보보호법, 정보통신망 이용 및 촉진에 관한 법률 등 정보보호 관련 법상 개인정보처리의 “제3자 제공”과 “위탁”의 개념 차이를 살펴볼 것이다. 그리고 “위탁”과 달리 핀테크 기업처럼 “제3자 제공”, 즉 일반적으로 “제휴” 관계인 경우 제공하는 기업의 법적 의무가 지나치게 완화되어 있는데 반해 정보유출 위험은 상대적으로 높기 때문에 현실에 맞는 정보보호 관련 법제도 정비를 제언하고자 한다.

또한 “제3자 제공”시 제공받는 기업이 스스로 정보보호 수준을 높일 수 있도록 정보보호 자가진단 체크리스트를 제시한다. 이를 통해 금융회사 오픈 플랫폼을 활용하는 31개 핀테크 기업을 진단한 결과, 수탁자보다 정보보호 수준이 상대적으로 미흡하다는 것을 확인하였다. 금융회사와 “제3자 제공” 관계인 핀테크 기업의 정보보호 수준이 높아질 수 있도록 체크리스트의 적극적인 활용을 제언한다.

ABSTRACT

It is actively opening the market to fintech companies through open platforms, such as financial institutions and public institutions. In this thesis, we will look at the conceptual differences between the “provision of third-party information” and “entrustment” of information protection related laws, such as the Personal Information Protection Act, the Act on Promotion of Information and Communications Network Utilization and Data Protection Etc (Network Utilization Protection Act). In addition, the legal obligation to provide information regarding the legal rights of information is considered to be relevant, whereas the legal obligation of the private information provided by the company is excessively mitigated, whereas the legal obligation of the company to provide information is excessively mitigated. In addition, I suggest self-diagnosis checklist to help fintech companies improve their privacy levels. It was found that the level of information protection was relatively insufficient compared to the consignees based on the results of a survey conducted for 31 fintech companies. Aggressive use of the checklist is suggested to raise the level of information protection for those companies.

키워드 : 사이버보안, 위험평가, 정보보호, 핀테크
Cybersecurity, Security Risk Assessment, Information Protection, Fintech

* First Author, Graduate School of Information Security, Korea University(joeny@korea.ac.kr)
** Corresponding Author, Graduate School of Information Security, Korea University(iskim11@korea.ac.kr)
Received: 2017-07-26, Review completed: 2017-09-26, Accepted: 2017-10-20

1. 서 론

최근 금융권 최대 화두는 핀테크라고 할 수 있다. 스마트폰 이용자가 매년 급격히 증가함에 따라 모바일 결제 시장도 급성장을 거듭하고 있다[19]. 이에 따라 기존 금융회사 고유 업무의 일부가 기능별로 분할되어 대출, 모바일 송금 등의 업무를 핀테크 기업들이 수행하고 있는 현상이 점차 확산되고 있다[13].

이러한 핀테크 시장 활성화에 부응하여 금융회사는 보유하고 있는 정보를 오픈 플랫폼(Open platform)을 통해 API(Application Programming Interface) 방식을 이용하여 핀테크 기업에게 개방하기 시작했다. 2016년 8월에는 금융결제원을 중심으로 16개 은행이 참가한 은행권 공동 오픈 플랫폼 서비스가 시작되었고, 일부 금융회사들은 개별적으로 오픈 API를 적극 활용하고 있다.

하지만 핀테크 시장이 활성화되고 있는 긍정적인 이면에는 개인정보 침해사고도 증가하고 있다는 부정적인 면도 상존한다. <Table 1>은 한국인터넷진흥원으로 접수된 개인정보 침해신고 접수 건수 추이를 나타낸다[12]. 개인정보를 수집한 목적 외의 이용 또는 제3자 제공 관련한 신고는 2014년 이전 3천 건 이하였으나, 이후 3천 건이 넘게 접수되었다.

금전을 직접 다루는 금융회사들은 수차례의 정보유출, 해킹 등 침해사고를 겪고 나서 개인정보보호법, 전자금융거래법, 신용정보의 이용 및 보호에 관한 법률 및 관련 고시 제·개정을 통해 매우 구체적이고 정교한 보안 조치를 해왔다. 특히 전자금융감독규정에서 정한 사항을 이행하기 위하여 정보보호최고책임자(CISO)의 임원급 지정과 더불어 정보보호 관련 인력과 예산을 정보기술(IT) 부문 대비 일정 수준 이상을 초과하여 확보하는 등 다른 업종에 비하여 정보보호 수준이 높은 편이다. 이는 <Table 2> 개인정보보호 실태조사 보고서에서 금융/보험업 종사자가 정보보호 관련 의무사항에 대해 정확히 인지하고 있다고 응답한 비율이 73%로 타 업종 대비 가장 높다는 것만 봐도 알 수 있다[16].

하지만 금융회사와 달리 금융서비스를 제공하는 핀테크 기업들은 대부분 5명 내외의 직원으로 구성된 스타트업으로써 정보보호 수준은

〈Table 1〉 Number of Inventions to Report Personal Information Violation Using it Rather than Original Purposes〔12〕

Year	2012	2013	2014	2015	2016
Number of cases	2,196	1,988	2,242	3,585	3,141

〈Table 2〉 Recognition of Duty on Provision of Personal Information Processing to a Third-Party〔16〕

area	Well-known	Have heard of	Don't know.
Banking/Insurance	73.0%	23.8%	3.2%
Health/Welfare	65.8%	31.9%	2.3%
Electricity/Gas/Water	61.9%	33.3%	4.8%
Private education	47.2%	45.4%	7.4%
Real Estate/Lease	46.0%	40.3%	13.7%
Information/ Communication	42.7%	42.6%	13.7%
Association/Group	42.8%	49.2%	8.0%
Manufacturing	34.3%	52.4%	13.3%
Distribution/ Logistics/wholesale	31.7%	50.8%	17.5%
Accommodation/ Restaurant	23.7%	46.5%	29.8%

상대적으로 매우 낮을 수밖에 없을 것이다. 이는 앞서 살펴본 개인정보보호 실태조사 보고서에서 개인정보보호법 인지여부를 묻는 질문에 잘 안다고 답한 경우가 300명 이상 기업이 80.7%인데 반해 5명 미만 기업은 34.6%에 그쳤다는 것을 통해 유추해볼 수 있다[17]. 적은 인원으로 운영되는 기업일수록 상대적으로 정보보호에 소홀할 수 있다는 것을 의미하며, 스타트업 위주인 핀테크 기업을 통한 정보 유출 위험을 중요하게 다루어야 한다는 것을 보여주는 수치이기도 하다.

〈Table 3〉 Recognition of PERSONAL INFORMATION PROTECTION ACT based on Number of Employees〔17〕

Number of Employees	Well-known	Have heard of	Don't know.
Less than 5	34.6%	56.4%	8.9%
5~49	56.1%	40.9%	3.0%
50~299	69.4%	29.7%	0.9%
Over 300	80.7%	17.5%	1.8%

그 동안 개인정보 수탁자에 대한 연구는 많이 되어 왔지만, 이와 달리 개인정보보호법의 "제3자 제공"에 대해서는 고객의 동의를 기반으로, 제공받는 자가 스스로 관리책임을 갖게 되므로 연구가 부족했던 것으로 보인다. 그리고 금융회사들이 개인(신용)정보 업무와 관련하여 "위탁"과 "제휴"의 구분이 명확치 않아 보수적으로 해석하는 등 혼란을 초래하여 감독당국에 관련 해설서를 요청[1]하는 경우도 종종 있는 것으로 보아 여전히 두 가지의 구분이 실무적으로 모호하다고 할 수 있다. 또한 개인정보보호법과 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 "정보통신망법"이라 한다)에서 정한 개인정보의 "제3자 제공"과 "위탁"의 구별에 관한 법리를 원심에서 오해하고 필요한 심리를 다하지 아니했다고 언급한 대법원 판결 2016도13263[6]의 경우만 봐도 명확한 구분이 어렵다는 것을 증명한다.

본 연구에서는 개인정보 처리 "위탁"과 "제3자 제공" 관련 법상 분류에 따른 문제점을 살펴볼 것이다. 또한 구체적인 핀테크 기업에 대한 정보보호 수준 진단 기준을 제시하고, 실제 핀테크 기업에 대한 진단 결과를 확인해볼 것이다. 이를 토대로 실무를 반영한 개선방안을 제시함으로써 궁극적으로 스타트업의 정보보호 수준을 높이는데 기여하여, 보다 넓게는 핀테크 시장의 활성화를 도모하고자 한다.

2. 개인정보 처리 위탁 및 제3자 제공의 개념

2.1 위탁과 제3자 제공 관련 법률

개인(신용)정보의 처리 "위탁"과 "제3자 제공"의 구분은 개인정보보호법, 신용정보의 이용 및 보호에 관한 법률(이하 "신용정보법"이라 한다), 정보통신망법에 명시되어 있다.

개인정보보호 법령 및 지침·고시 해설에 따르면 "위탁"과 "제3자 제공"은 모두 개인정보가 다른 사람(제3자)에게 이전되거나 공동으로 처리하게 된다는 측면에서는 동일하지만, 개인정보를 제공하는 자의 업무 목적과 이익을 위한 경우 "위탁"이고, 개인정보를 제공받는 자의 업무 목적과 이익을 위한 경우 "제3자 제공"으로 해설하고 있다[15]. 즉, 해당 업무가 누구의 목적

과 이익을 위한 것인지가 가장 핵심적인 구분 기준이라는 것을 알 수 있다. 동일하게 금융분야 개인정보보호 가이드라인에도 해당 업무의 목적과 이익을 누가 취하는지 여부에 따라 “위탁”과 “제3자 제공”을 구분하고 있다[2]. 상기내용을 종합하여 개인(신용)정보의 “위탁”과 “제3자 제공”을 구분하면 <Table 4>와 같다.

정보통신망법의 경우 개인정보 처리의 위탁 시에도 동의를 받아야 된다고 명문화하고 있다는 것이 개인정보보호법 및 신용정보법과 다른 부분이라고 할 것이다. 하지만, 동법 제25조 제2항에서 정보통신서비스의 제공에 관한 계약을 이행하고 이용자 편의 증진 등을 위하여 필요한 경우에는 고지절차 및 동의절차를 생략할 수 있다고 되어있는 점에서 결과적으로 다른 법률과 유사하다고 판단할 수 있다. 구체적으로 정보통신서비스 제공자를 위한 개인정보보호 법령 해설서에는 “위탁”과 “제3자 제공”의 본질적인 차이가 개인정보를 제공하는 자의 업무와 직간접적인 관련이 있는 경우 “위탁”이고, 관련이 없는 경우를 “제3자 제공”으로 본다고 해설 하였다[11].

〈Table 4〉 Classification of “Consignment of Personal Information Processing” and “Provision of Personal Information Processing to a Third-Party” as Required by Law

Area	Consignment of personal information processing	Provision of personal information processing to a third-party
The subject of the purpose of personal information and the purpose of the profit	A company that receives personal information	A company that provides personal information
Predictability	possible to predict by owner of information (in trusted range)	Difficult to predict by owner of information (out of trusted range)
Mandatory matters	Disclosure and notification of contents to owner of information Disclosure to Privacy Statement	separate agreement from owner of information Disclosure to Privacy Statement
Responsible for managing oversight and loss of liability	A company that provides personal information	A company that receives personal information
Legal provisions	PERSONAL INFORMATION PROTECTION ACT Article 26, USE AND PROTECTION OF CREDIT INFORMATION ACT Article 17, THE ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND DATA PROTECTION, ETC. Article 25	PERSONAL INFORMATION PROTECTION ACT Article 18, USE AND PROTECTION OF CREDIT INFORMATION ACT Article 32, THE ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND DATA PROTECTION, ETC. Article 24-2
example	Call Center(Help desk), TM outsourcing, Shipping, Operation of IT center operation	Credit card mileage objective carrier alliance, Delivers to an insurance company through an event
Relevance to the work provided by the provider	Part of the work involved directly or indirectly.	not involved directry or indirectly

2.2 위탁과 제3자 제공 관련 판례

대법원 판결(2011. 7. 14. 선고 2011도1960)에서 “제3자 제공”은 제공받는 자의 목적을 위하여 개인정보가 제공되는 경우이고, 타인 “위탁”은 제공하는 자의 사무 처리를 위한 경우로 구별하여야 한다고 하였다[4]. 또한 정보통신망법 제24조의 “제3자”의 범위에는 개인정보 취급을 위탁받은 수탁자는 포함되지 아니한다고 해석하였다는 점에 그 의의가 있다.

서울중앙지방법원 판결(2011. 9. 30. 선고 2008가 합49696)은 두 가지 형태로 구별하고 있는 입법 취지 등을 고려할 때, “위탁”은 제공하는 자의 업무와 직・간접적으로 관련된 업무 일부를 타인으로 하여금 그 책임과 권한으로 행하는 것을 의미하는 반면, “제3자 제공”은 제공하는 자의 업무와 직・간접적으로 관련이 없는 사항을 타인에게 제공하는 것을 뜻한다고 하여, 정보통신서비스 제공자를 위한 개인정보보호 법령 해설서의 내용과 정확히 일치한다[3].

2.3 위탁과 제3자 제공 관련 연구

정보통신망법 상의 ‘제3자 제공’과 ‘제3자 위탁’의 구별[18]은 위탁이 제3자 제공에 포함되는지 여부를 검토하고 개인정보의 침해 가능성 정도에 따라 구분한 정보통신망법의 내용이 타당하다고 판단하였고, 위탁에 비하여 제공하는 자의 관리감독 책임이 없는 제3자 제공이 개인정보의 오남용 가능성이 높다는 점을 지적하였다는 데에 그 의의가 있다.

개인정보보호 수탁사 관리체계 강화방안에 관한 연구[8]에서는 “위탁”과 “제3자 제공”의 사례구분을 통해 기업이 개인정보의 처리를 위탁할 경우 업무의 성격이 부수적인지 여부를 명확히 파악하는 것이 필요하다고 하였고, 위탁시 수탁자에 대해서는 철저한 관리・감독이 필요하다는 것을 검증하였다는 데 의의가 있다. 유사한 연구로써 개인정보보호 강화를 위한 위탁 업무 보안관리 프레임웍 제안[10]에서는 개인정보 처리의 생명주기별 고려해야 하는 정보보호 요건들을 제시함으로써 수탁자에 대한 관리강화의 필요성을 제시하였다.

업무위탁과 제3자 제공의 차이에 대한 올바른 이해[9]에서는 “위탁”과 “제3자 제공”의 차이에 대한 보다 구체적인 구분방법을 제시하고 있다. 최초의 본원적인 계약을 완성하기 위하여 부수적으로 제3자에게 제공하는 경우를 위탁으로 보고, 이와 달리 본원적인 계약과 관련이 없는 별개의 독립된 계약인 경우를 “제3자 제공”으로 판단하고 있다. 예를 들면 최조 금융회사와 고객이 예금거래를 위해 계약을

〈Table 5〉 Classification of Contract Relationship between “Consignment of Personal Information Processing” and “Provision of Personal Information Processing to a Third-Party”〔9〕

Area	Consignment of personal information processing	Provision of personal information processing to a third-party
Contractual relationship	An internal contract to complete the original contract	External contracts separate from original contracts
Independence of action	An act that depends upon the original contract	An act independent of the original contract

맺었고, 이를 유지하지 위하여 상담, 만기 안내 등을 위한 콜센터에 개인정보를 제공하는 것은 본원 계약을 위한 일종의 부수 업무로 보아 “위탁”으로 본다는 것이다.

핀테크 서비스의 개인정보보호 자가평가항목 개발에 관한 연구[7]에서는 핀테크 기업을 위하여 총 42개의 체크리스트를 제시하고 설문조사를 통해 그 필요성을 확인하였다. 이는 개인정보 처리의 “제3자 제공” 여부와 관계없이 핀테크 기업의 정보보호 강화방안이 필요하다는 데 공감대를 형성하였다는 점에 그 의미가 있다.

2.4 “위탁”과 “제3자 제공” 구분의 실익

기업이 개인정보 처리를 제3자에게 제공할 때 “위탁” 또는 “제3자 제공”의 법적 관계가 성립된다. 두 제공 방법을 구분하는 것이 실익이 있는지 해당 정보를 이용하는 자와 정보주체의 입장에서 각각 살펴보고자 한다.

개인정보를 취급하는 기업은 고객의 별도 동의없이 콜센터 등 “위탁”을 통해 효율적 업무 수행을 할 수 있다는 장점이 있다. 또한 다양한 사업을 영위하는 제3의 기업에 고객의 별도 동의를 전제로 정보를 제공함으로써 오픈 플랫폼과 같이 수수료 수익을 얻는 등 다양하게 개인정보의 활용도를 높일 수 있다. 이를테면 금융회사가 핀테크 기업에 고객의 개인정보를 제공함으로써 금전적 이득과 더불어 핀테크 생태계의 활성화까지 도모할 수 있는 것이다.

한편 개인정보를 제공하는 고객은 “위탁”과 “제3자 제공” 구분을 명확히 인식함으로써 “제3자 제공” 사항에 대하여 동의 또는 거부를 할 수 있어, 본인 정보에 대한 자기결정권을 강화할 수 있다 라는 측면에서 명백히 두 가지의 구분에 실효성이 있다고 볼 수 있을 것이다.

2.5 “위탁”과 “제3자 제공” 구분의 문제점

첫째, 용어 정의가 명확하지 않다. 관련법에서 별도로 용어 정의를 하지 않음으로 인해 개인정보의 제3자 제공이 위탁의 개념까지 포괄하는 개념으로 해석될 우려가 있다. 일반적으로 제3자 제공은 제휴 관계인 경우가 많아 “위탁”과 “제휴”로 구분하여 표기하기도 한다.

둘째, 두 가지 분류기준에 대한 해석이 명확하지 않다. 개인정보보호법과 동 법 해설서에는 <Table 4>에서 확인한 것과 같이 “위탁”과 “제3자 제공”은 제공 목적과 이익의 주체가 누구인지에 따라 분류하게 되어있다. 하지만 모든 계약은 양 당사자 간의 합의에 따라 서로가 이익이 되는 경우에 이루어지는 성질의 것이므로 상당히 추상적이라고 할 수 있다. 실무적으로 기업 담당자들이 가장 큰 혼란을 겪는 것이 이 부분이다. 예를 들어 금융회사의 오픈 플랫폼의 경우 금융회사는 개인정보 제공자로써 플랫폼 활성화를 통한 수수료 수익에 목적이 있고, 이를 이용하여 신규 서비스를 제공하는 핀테크 기업은 자신만의 서비스를 통해 수익 창출에 목적이 있는 것처럼 양 당사자가 각자의 목적과 이익이 다르게 존재한다는 점을 간과하고 있다.

최초 계약과의 직・간접적 연관성을 잣대로 구분하는 정보통신망법 해설서의 내용이 이 부분에 대한 가장 정확한 법리적 해석이라고 할 수 있으나, 이와 다르게 깨알고지 사건으로 알려진 대법원 판결에서는 두 항목을 명확히

구분하기 위해서 고려해야하는 5가지 사항을 제시하였다[5].

(1) 개인정보의 취득 목적과 방법
(2) 대가 수수 여부
(3) 실질적인 관리·감독 여부
(4) 개인정보보호 필요성에 미치는 영향
(5) 개인정보 이용 필요가 있는 자가 실질적으로 누구인지 고려

개인정보의 제공 목적과 이익의 주체를 기본 기준으로 정하되, 제공하는 자가 관리·감독을 실질적으로 수행하였고 대가수수 등이 있다면 "제3자 제공"이 아닌 "위탁" 관계로 판단하는 것이 적절하다고 함으로써 오히려 법해석에 대한 혼란을 다소 야기하고 있다.

셋째, 개인정보의 "위탁"에 비해 "제3자 제공"의 경우 개인정보를 제공받은 기업이 핀테크 스타트업과 같이 소규모로 이루어진 경우 정보보호 수준이 낮아 정보의 오남용 또는 유출 사고 발생 가능성이 높다. 구체적인 정보보호 수준은 실제 현장 진단 결과를 통해 다음 장에서 확인해볼 것이다.

"위탁"인 경우에는 원 계약의 연장선상의 업무로 보고 개별적으로 정보주체의 동의를 받을 필요 없이 홈페이지 등에 게재하고 수탁자에 대하여는 교육, 점검 등 관리감독 의무를 이행하여야 한다. 구체적으로 개인정보보호법 제26조제6항과 정보통신망법 제25조제5항에는 수탁자의 법 위반으로 손해배상책임이 발생한 경우 위탁자의 소속 직원으로 본다고 함으로써 보다 적극적인 수탁자에 대한 위탁자의 관리·감독 의무 이행을 요구하고 있다. 따라서 수탁자는 그 기업의 인력, 자산 규모에 관계없이 계약과 동시에 위탁자라는 제3의 관리주체가 생성되고, 수탁자 스스로 개인정보의 안전한 관리를 함과 동시에 위탁자의 교육과 점검을 받는 구조로 정보보호 수준을 한층 더 높일 수 있는 시스템이 되어있는 것이다.

〈Table 6〉 Judicial Precedent about Classification of "Consignment of Personal Information Processing" and "Provision of Personal Information Processing to a Third-Party"〔5〕

Area	Key contents
Fact	◦ Contract for selling customers' personal information submitted through a giveaway event to insurance companies ◦ Obtain customer consent by specifying the contents of the personal information collection and providing the contents with 1mm big. ◦ Provide personal information to insurance companies for accurate marketing target selection
Original Judgement (Not guilty)	◦ Include all items that must be notified to the customer ◦ Preceding marketing targets is simply consignment of personal information processing to insurance companies
Judgement by supreme Court	◦ Obtained consent from customers using personal information either in false or other unjust means - To hide the main purpose of a prize event and collect irrelevant personal information - Refusing to provide service to customers who disagree ◦ It is "Provision of personal information processing to a third-party" not "Consignment of personal information processing" - Insurance companies received personal information for their own interests and business processes. - Companies providing personal information did not manage and supervise insurance companies.

하지만 “제3자 제공”의 경우는 고객의 직접적인 동의를 전제조건으로 개인정보를 제공받는 자 스스로 개인정보를 준수하기 위한 다양한 노력을 해야 한다. 제공하는 자가 제공받는 자에 대한 법상 관리・감독 의무가 전혀 없기 때문이다. 본 연구에서 조사된 핀테크 스타트업의 정보보호 수준은 수탁자에 비하여 낮음을 알 수 있었다. 즉, 동일한 개인정보가 소규모 기업인 제3자에게 제공된다고 가정할 때 “제3자 제공”인 경우가 “위탁”인 경우에 비해 개인정보 유출 위험이 더 높을 수 있다는 것을 의미한다. 위탁자의 점검과 교육의 효과를 무시할 수 없기 때문이다.

3. 제3자 제공시 제공받는 기업의 정보보호 강화 방안

앞서 살펴본 바와 같이 개인정보의 “제3자 제공” 시에는 제공받는 자에 대한 제공하는 자의 관리・감독 책임이 없기 때문에 “위탁”에 비하여 제공받는 자가 정보보호에 소홀할 수 있다고 하였다. 이 장에서는 “제3자 제공”시 정보보호 관리를 강화하기 위한 법률 개선안과 진단 체크리스트를 제시하고자 한다.

3.1 제3자 제공시 정보보호 관련 법률 및 제도 개선방안

첫째, 용어 정의의 혼돈을 막기 위해 관련 해설서와 가이드라인에 “위탁”과 “제3자 제공”의 구분을 명확히 할 필요가 있다. 원 계약의 이행을 위한 부수적인 계약이면 “위탁”으로, 그렇지 않고 원 계약과 관련이 없는 새로운 계약이면 “제3자 제공”임을 명시할 필요가 있는 것이다. 이는 고객의 동의가 필요한지 여부와 직결되므로 중요한 사항이다. 용어의 명확한 설명이 없어 혼돈을 불러일으킨 것이 두 제공방법의 구분을 어려워하는 가장 큰 이유이다.

둘째, “위탁”과 “제3자 제공”의 구분과 관련 없이 개인정보를 제공받는 자에 대한 제공하는 자의 관리・감독을 의무화시키지 않고, 제공하는 자의 자율에 맡기되 사고 발생 시 손해배상 책임을 가중하여 묻는 방법이 있다.

이 경우 핀테크 기업과 같이 정보보호 수준이 낮을 것으로 예측되는 소규모 기업에 대하여는 제공하는 자가 정보보호 교육을 실시하고 현장점검을 실시하는 등 제공된 개인정보의 안전성 확보를 통해 제공받는 자의 정보보호 수준 향상에 직접 관여할 수 있다. 또한 제공받는 자의 정보보호 관리체계 수준이 이미 일정수준 이상으로 높은 경우 직접적인 관리・감독 보다는 개인정보 유출배상 책임보험에 가입할 것을 양 당사자 간의 계약서에 명시하는 등 자율적 보안이 이루어질 수 있도록 시장 환경을 조성해야 한다.

셋째, “제3자 제공” 시 해당 서비스를 이용하기 위해서는 고객의 사전 동의가 반드시 필요하다. 이때 고객 동의절차 단계에서 해당 기업의 정보보호 관리체계 수준을 확인할 수 있도록 구체적인 정보를 제공할 필요가 있다.

<Table 7>과 같이 현행 법률에서 정한 개인정보 처리방침을 비교 분석해보면 개인정보보호법과 정보통신망법의 내용은 대동소이하나, 정보통신망법과 달리 개인정보보호법 제30조에는 개인정보의 안전성 확보조치에 관한 사항을 기재하도록 의무화하고 있다.

〈Table 7〉 Privacy Policy

Area	PERSONAL INFORMATION PROTECTION ACT	NETWORK UTILIZATION PROTECTION ACT
similar	Purpose of processing	Purpose of Collection and Utilization
	Processing and Retention Period	Retention and utilization period
	Consignment/ provision to a third-party of personal information processing	Consignment/ provision to a third-party of personal information processing
	Rights, duties and execution methods	Rights and execution methods
	Personal information items that are processed	Personal information items collected, how to collect
	Destruction	Destruction procedures and methods
	CPO, Requisition request processing department	CPO, Grievance settlement department
different	Violation of Rights and Protection of data subject	The installation and operation of the device collecting automatically the personal information like the Internet logon files, etc. and how to deny such device;
	Changed history of privacy policy	
	secured safeguards	

하지만, 다음 장의 조사대상 핀테크 기업뿐만 아니라 대다수의 기업들은 안전성 확보조치 항목에 대해서 해킹 등 대비책과 직원 교육 등 일반적 의무사항만 나열했을 뿐, 해당 기업의 정보보호 수준을 판단할 수 있는 충분한 정보를 제공하고 있지는 않았다.

한편, 정보보호 산업의 진흥에 관한 법률에 따른 정보보호 공시제도의 공시 항목은 <Table 8>과 같이 4가지로 구분된다. 이는 전자금융거래법상 일정규모 이상의 금융회사가 준수해야하는 예산 및 인력 투자 현황을 포함하며, 정보보호 관련 인증, 평가, 점검 관련 사항과 더불어 기타 정보보호를 위한 활동도 포함하도록 되어있다.

〈Table 8〉 Information Protection Publication within INFORMATION PROTECTION INDUSTRY PROMOTION Act

No	Disclosure item
1	Investment in information protection against investment in information technology
2	Number of employees in information protection against employees in information technology
3	Items related to authentication, evaluation, and inspection of information protection(If applicable)
4	Activities of Information Protection for the Protection of Information Using Information Services

이를 활용하여, 개인정보 처리방침에 정보보호 공시제도에 포함된 4가지 항목을 기본적으로 포함하도록 하고, 고객의 사전 동의 절차에 반드시 개인정보 처리방침을 확인할 수 있도록 의무화 하는 것을 고려해볼 수 있다. 정보보호를 위한 인력과 예산이 얼마나 투입되고 있는지에 대한 정보를 고객에게 제공함으로써 자기결정권을 보장함과 더불어 핀테크 기업들도 정보보호 수준을 향상시킬 수 있는 긍정적 효과를 기대할 수 있을 것이다.

3.2 제3자 제공 기업 정보보호 체크리스트

스타트업 위주인 핀테크 기업은 인력과 비용의 문제로 정보보호 관리체계 인증을 받기 어려운 것이 현실이다. 이러한 기업을 위한 간소화된 ISMS(정보보호관리체계) 또는 PIMS (개인정보보호관리체계) 인증제도의 마련도 필요하며, 정보를 제공하는 개개인이 서비스를 제공하는 기업을 신뢰할 수 있는 기반이 되는 정보보호 제도를 활성화 할 필요가 있다.

그 예시로 본 연구에서는 핀테크 기업을 위한 간소화된 정보보호 자가점검 체크리스트를 <Table 9>와 같이 제시하고자 한다. 해당 체크리스트는 인증 적용 유형을 공공, 대기업, 중소기업, 소상공인으로 분류해서 적용하고 있는 PIMS 인증제도를 기반으로 작성되었다. 소기업 및 소상공인지원을 위한 특별조치법 시행령에 따르면 광업, 제조업, 건설업 및 운수업은 상시 종업원수가 10명 미만인 경우, 그 밖의 업종은 5명 미만인 경우를 소상공인으로 정의하고 있고, 특히 핀테크 기업들은 10명 미만인 경우가 대다수로 소상공인 유형에 해당하는 인증항목을 기준으로 기업 스스로 체크해보고 개선할 수 있도록 간소화하였다. PIMS 소상공인 인증항목 총 47개 중 “개인정보의 이전”, “간접수집 보호조치” 등 성격상 핀테크 기업 대부분에게 적용되지 않는 항목과, 핀테크 기업에게 제공하지 않는 고유식별정보 관련 항목을 제외시켰고, 일부 항목은 통합하였다. 또한 서비스 가용성 확보를 위한 백업 항목은 추가하였다. 이 결과 체크리스트는 관리적 보안 5개, 기술적 보안 13개, 물리적 보안 2개, 총 20개의 정보보호 준수사항으로 재구성하여 핀테크 기업이 쉽게 접근할 수 있도록 적용해보았다.

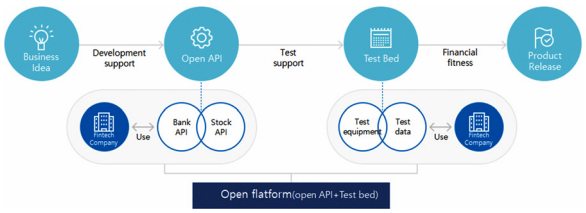
4. 핀테크 기업 정보보호 진단결과

금융회사의 오픈 플랫폼의 개념과 실제 API를 통해 개별 서비스를 제공하는 핀테크 기업 현황을 분석해봄으로써 앞에서 언급한 개인정보의 “위탁”과 “제3자 제공”의 분류를 적용해 보고자 한다.

4.1 오픈 플랫폼 개요

오픈 플랫폼이란 금융회사가 제공하는 다양한 API 서비스를 핀테크 기업이 자유롭게 조합하여 새로운 서비스를 고객에게 제공하는 제반 인프라를 의미한다.

2016년 8월에 공식 출범한 “은행권 공동 OPEN 플랫폼”의 경우 금융결제원이 플랫폼을 제공하고 16개의 참가은행이 총 5가지의 API(잔액조회, 거래내역조회, 계좌실명조회, 입금이체, 출금이체)를 제공하고 있다. 핀테크 기업은 이 API를 이용하여 사업 아이디어를 웹(Web)이나 앱(App) 형태의 다양한 서비스로 고객에게 제공 가능한 것이다.

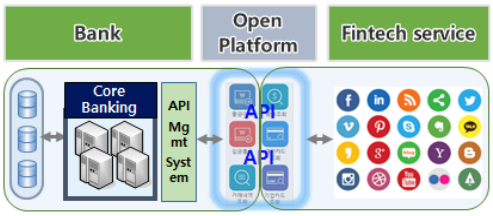


〈Figure 1〉 Process of Using Open Platform

〈Table 9〉 Information Protection Checklist for Fintech Companies

area		No.	Check item	Law & Regulation
Managerial	Organization configuration	M1	Designated information security officer?	PI ACT §31 NU ACT §27, §45-3
	Regulations and guidelines	M2	Established an internal provision of information protection?	NU ACT §28
	Information Protection Education	M3	Are information protection education plans established annually and implemented?	PI ACT §28 FS Regulation §19-2
	Consent for using personal information	M4	Agreed to the collection, utilization, and utilization of personal information?	PI ACT §15 NU ACT §27-2
	Written oath	M5	Receiving a pledge or a confidentiality oath from the employees and the outside party?	PI ACT §29 NU ACT §45 FS Regulation §13
Technical	Managing access rights	T1	Managing system access authorization and deletion records	PI ACT §29 NU ACT §45 FS Regulation §13
	Access records management	T2	Managing system access records?	PI ACT §29 NU ACT §28 FS Regulation §13
	Password complexity	T3	Are the organization's password minimum length and complexity settings enforced?	PI ACT §29
	Network security	T4	Is there a proper system for network security? such as firewall, IDS	PI ACT §29 NU ACT §28
		T5	Is restricted to allow access to computers only in certain PCs? and is there a secure means of access when accessing the system from outside?	PI ACT §29 NU ACT §28
	Server management	T6	Is the organization preparing access controls for key equipment such as servers?	PI ACT §29 NU ACT §28
		T7	Is the organization providing protection measures for the public web server?	PI ACT §24
	Backup management	T8	Establishing and implementing backup and recovery procedures?	FS Regulation §13
	Encryption	T9	Are key information encrypted with a secure algorithm?	PI ACT §24 NU ACT §28
		T10	Does the organization establish and implement a secure key management procedure?	FS Regulation §31
	Terminal security	T11	Is the terminal secure solution installed and performing the latest updates?	PI ACT §29 NU ACT §28 FS Regulation §16
		T12	Using boot and login password correctly?	PI ACT §29 NU ACT §28
	Vulnerability check	T13	Is a vulnerability check conducted once a year?	PI ACT §29 NU ACT §45-3
Physical	Protected zone designation	P1	Are protective zones designated for protection of major systems and implementing protective measures?	PI ACT §29
	Access Control	P2	Does the organization prepare access control procedures and manage access records?	PI ACT §29

1) PI ACT: PERSONAL INFORMATION PROTECTION ACT.
2) NU ACT: THE ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND DATA PROTECTION, ETC.
3) FS Regulation: ELECTRONIC FINANCIAL SUPERVISORY REGULATION.



〈Figure 2〉 Conceptual Diagram of Open Platform

4.1.1 A금융회사 제공 OPEN API 현황

본 연구에서는 상세한 검토를 위해 총 60개의 다양한 API를 제공하는 A금융회사의 오픈 플랫폼 사례를 웹 사이트에 공개된 정보를 통해 확인해보았다. A금융회사가 제공하는 API는 금융 API, 제휴 API, 서비스관리 API 3가지로 구분되며 현재 금융, 서비스관리 기능을 제공하는 60개의 API가 운영되고 있다. A사와 핀테크 기업간 관리 목적의 API는 전문 상에 개인신용정보를 포함하고 있지 않으며, 개인정보보호법상 개인신용정보로 분류되는 주민등록번호, 계좌번호, 고객명, 거래내역, 카드번호, 생년월일을 포함하고 있는 금융 API는 총 25개이다.

몇 가지 API 전문 상세내역을 보면, A금융회사와 핀테크 기업 간에는 고객의 계좌번호와 1대 1로 매칭되는 사전 약속된 임의번호가 있다. 예를들어 “잔액조회” API는 핀테크 기업이 사전에 약속된 임의번호를 입력하면 A금융회사는 고객의 계좌 잔액과 실제인출 가능금액을 응답한다. “개인카드 한도조회” API는 핀테크 기업의 서비스 이용고객이 현금서비스 잔여한도, 해외이용한도, 해외 ATM 잔여한도, 카드 결제일, 체크카드여부를 A금융회사로부터 확인할 수 있도록 전문이 구성되어 있다.

4.2 금융회사 OPEN 플랫폼 이용기업

4.2.1 OPEN API 이용 핀테크 기업현황

2017년 4월 기준으로 A금융회사가 제공하는 API를 활용하고 있는 31개의 핀테크 기업 현황을 조사해보았다.

〈Table 10〉 Status of Fintech Companies Using Open Platform

Number of employees		Number of companies	Ratio
1~9		24	77.4%
	1~3	4	16.7%
	4~6	15	62.5%
	7~9	5	20.8%
10~19		5	16.1%
20~29		1	3.2%
over 30		1	3.2%

먼저 <Table 10>의 기업규모를 살펴보면 31개 기업 평균 8.3명의 임직원이 있었고, 10명 미만인 기업이 24개로 전체의 77.4%를 차지하고 있다. 세부적으로는 4명에서 6명의 임직원이 있는 기업이 15개로 가장 높은 비율을 차지하고 있는 것을 알 수 있다. 2016년 대한민국 핀테크 기업 전체 평균 종업원 수가 19.7명이며, 그 중 핀테크 전문 인력은 4.8명으로 조사된 바 있다[10]. 스타트업인 핀테크 기업은 주로 10명 내외의 소규모 형태로 구성되어있음을 알 수 있다.

<Table 11>은 핀테크 기업들이 제공하는 서비스 현황이다. 20개 기업이 주로 입금, 출금 API를 활용하여 P2P 대출 또는 결제・송금 서비스를 제공하고 있다.

〈Table 11〉 Status of Fintech Services Using Open Platform

Key services	Number of companies
P2P loans	12
Simple Payment and Remittance	8
Easy book	4
Card slip processing	1
Other brokerage business	6

4.2.2 핀테크 기업에 대한 금융회사의 정보보호 관련 법상 의무

앞서 살펴본 바와 같이 핀테크 기업은 오픈 플랫폼을 통해 보다 다양한 서비스를 고객에게 제공할 수 있게 되었다. 하지만 금융회사 입장에서 서비스를 개방하고, 고객의 금융거래정보를 제공한다는 것은 여간 부담이 아닐 수 없을 것이다.

개인정보보호법과 정보통신망법 및 은행연합회 개인정보보호 가이드라인을 기준으로 <Table 4>와 <Table 5>의 기준에 따라 위탁과 제3자 제공의 분류를 대입해보면 개인정보 제공의 목적은 단순히 수수료를 받는 A금융회사가 아니라 고객에게 직접 서비스를 제공하는 핀테크 기업의 목적과 이익에 더 부합하므로 “제3자 제공”이라고 분류하는 것이 합당하다고 할 수 있다.

“제3자 제공”이기 때문에 금융회사는 고객으로부터 정보제공에 대한 사전 동의를 반드시 받아야 하고 이를 개인정보 처리방침을 통해 인터넷 홈페이지 등에 공개하여야 하는 의무가 발생한다. 그렇게 때문에 고객이 오픈 플랫폼을 활용한 핀테크 서비스를 이용하기 위한 첫 번째 단계로써, A금융회사에 ARS를 통해 본인 인증과 개인정보 제공에 동의하는 절차를 밟게 되어있는 것이다. 동의 절차 이후에 A금융회사는 정보보호 관련 법상 개인정보 처리방침 공개 이외의 추가적인 의무가 발생하지 않는다. 핀테크 기업에 대한 점검과 교육은 법률상 위탁 관계가 성립되어야 발생하는 의무이기 때문이다.

4.3 핀테크 기업 정보보호 진단결과

A금융회사는 오픈 플랫폼을 통해 API를 활용하여 새로운 서비스를 제공하는 핀테크 기업에 대한 점검 의무는 명백히 존재하지 않는다. 하지만 핀테크 기업이 제공하는 서비스에 대한 해킹 등 침해사고가 발생하는 경우 A금융회사의 평판리스크에도 영향을 미치게 될 것은 분명하다.

예를 들어 P2P 대출 핀테크 서비스가 해킹되어 거액의 대출이 발생하였는데, 이 대출금이 고객이 원하는 계좌가 아닌 대포통장 등 타인명의의 계좌로 이체되는 경우가 있을 수 있다. 이 경우 고객은 핀테크 기업은 물론 대출을 일으킨 A금융회사에게도 책임을 전가할 우려가 있을 수 있다. 그렇기 때문에 오픈 플랫폼은 이체금액과 횟수를 제한하는 등 여러 가지 보안장치를 해두고 있는 것으로 확인되었다.

따라서 핀테크 기업이 기본적인 정보보호 관리체계를 보유하고 있는 경우에 한하여 오픈 플랫폼을 이용가능토록 하는 것이 바람직하다는 결론을 도출할 수 있었다. 구체적으로 핀테크 기업의 정보보호 실태를 확인한 현장조사 결과를 살펴보자.

4.3.1 조사 방법

2016년 4월부터 2017년 4월까지 31개의 핀

테크 기업의 정보보호 실태에 대해 현장조사를 실시하였다.

현장 조사는 IT 및 정보보호 경력 10년 이상이며, 정보보호 관리체계 국제인증심사원 자격증 보유자와, 국제공인 정보보호 관련 자격증 등을 보유하고 있는 A금융회사 직원이 직접 실시하여 핀테크 기업 간의 정보보호 수준을 객관적으로 비교할 수 있도록 하였다.

4.3.2 조사 결과 요약

체크리스트 20개 항목으로 서면점검 이후 현장점검 결과 결함이 전혀 없는 기업은 단 한 군데도 없었고, 11개 이상 미흡한 기업이 13개로 전체의 41.9%를 차지할 정도로 정보보호 수준이 미흡한 것으로 확인되었다.

〈Table 12〉 Total Defect Count Result

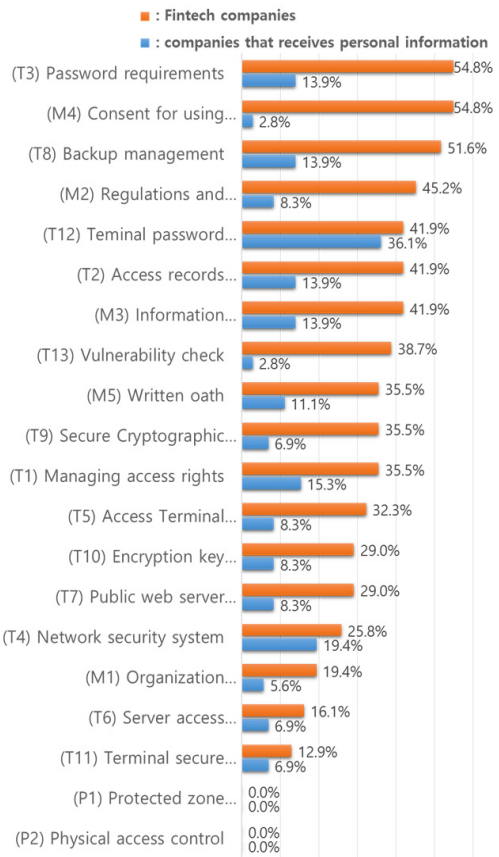
Total defect count	Number of companies	Ratio
0~5	10	32.3%
6~10	8	25.8%
11~15	9	29.0%
16~20	4	12.9%

다만, 해당 핀테크 기업들은 미흡사항이 전수 조치 완료된 이후에 대고객 서비스를 오픈할 수 있게 계약이 되어있고, 실제 이행점검 결과 이상 없는 기업만이 서비스를 제공하고 있다는 점에서 정보보호 리스크는 낮아졌음을 염두에 두어야 한다. 하지만 서비스를 준비하는 단계에서의 정보보호 실태를 살펴봄으로써, 일반적인 소상공인의 정보보호 수준을 미루어 짐작해볼 수 있다는 점에서 세부 결과를 확인해볼 필요가 있다.

4.3.3 조사 결과 개선 필요사항

A금융회사는 개인정보 처리 수탁자에 대하여 교육 및 점검을 실시하여 정보보호 관련법상 의무 이행을 도모하고 있다. 구체적으로 2016년 수탁자 점검결과와의 비교를 통해 객관적인 핀테크 제휴사의 정보보호 수준을 확인해보았다.

<Figure 3>과 같이 체크리스트 20개 항목 가운데 물리적 보안 2개 항목을 제외하고 전부 수탁자보다 핀테크 기업이 미흡하였다.



〈Figure 3〉 Survey Results of Fintech Companies' Information Protection Status

미흡건수가 많은 순서대로 확인해보면 시스템의 비밀번호 설정 시 최소길이 및 복잡도 설정을 강제화하고 있지 않고 있는 핀테크 제휴사가 54.8%로 과반을 차지하는데 비해, 개인정보 처리 수탁자는 13.9%로 준수율에 있어 큰 차이를 보이는 것을 확인할 수 있다.

방송통신위원회의 개인정보의 기술적, 관리적 보호조치 기준 제4조에 따르면 비밀번호는 영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상으로 설정하거나, 3종류 이상을 조합하여 최소 8자리 이상의 길이로 복잡도를 설정하도록 예시하고 있다. 시스템 최초 설정 시 기본 비밀번호를 변경하여야 함은 물론이고, 반기 1회 이상 변경하는 것도 정보보호 강화를 위해 반드시 조치되어야 하는 필수항목이다.

〈Table 13〉 Complied with Password Requirements(T3)

Subject	Number of compliant companies	Number of noncompliant companies	Noncompliant ratio
Fintech companies	14	17	54.8%
consignee	62	10	13.9%

또한, 개인정보 수집 시 동의절차를 적절히 이행하지 않은 핀테크 기업은 54.8%로 수탁자(2.8%)에 비해 미준수율이 월등히 높았다.

〈Table 14〉 Consent for Using Personal Information(M4)

Subject	Number of compliant companies	Number of noncompliant companies	Noncompliant ratio
Fintech companies	14	17	54.8%
consignee	70	2	2.8%

개인정보보호법 제15조에는 개인정보처리자가 개인정보를 수집·이용할 경우 필요한 사항이 열거되어 있다. 일반적으로 정보주체의 동의를 받아야 하며, 이 경우에도 목적에 필요한 최소한의 정보만 수집하여야 한다. 이 항목은 기본적인 정보보호 관련법에 대한 핀테크 기업의 대비 수준이 부족하다는 것을 알 수 있는 중요한 항목이라고 할 수 있다.

백업 대상, 주기, 방법, 절차 등이 포함된 백업 및 복구절차를 수립·이행하지 않고 있는 핀테크 기업의 비율은 전체의 51.6%로 수탁자 미준수율 13.9%에 비해 높은 것을 알 수 있다.

〈Table 15〉 Backup Management(T8)

Subject	Number of compliant companies	Number of noncompliant companies	Noncompliant ratio
Fintech companies	15	16	51.6%
consignee	62	10	13.9%

전산장애나 침해사고 등으로 인한 서비스 가용성을 확보하지 못하면 핀테크 기업의 신뢰성에 큰 영향을 미칠 수 있는 중요한 사항이다. 핀테크 기업과 같은 스타트업은 정보자산 보호를 위한 예산 확보가 어려울 수 있으므로 IDC 센터의 클라우드 서비스를 이용하는 것도 하나의 방법이 될 수 있다.

5. 결 론

<Figure 3>에서 오픈 플랫폼을 활용하고 있는 핀테크 제휴사가 개인정보 처리 수탁자

에 비해 기본 정보보호 준수사항을 이행하지 못하는 비율이 상당히 높다는 것을 확인하였다. 이는 <Table 3>에서 살펴본 바와 같이 임직원 수가 적을수록 개인정보보호법상 의무를 인지하지 못할 확률이 높다는 설문조사 결과와 일맥상통한다고 볼 수 있다.

일률적으로 개인정보 처리 위탁과 제3자 제공이라는 법상 구분을 통해 개인정보를 제공받는 자에 대한 제공하는 자의 관리감독 의무를 부과하는 것은 지금의 핀테크 시대에 적절치 않다. 이를 개선하기 위하여 제3자 제공시 제공받는 기업의 정보보호 강화 방안을 앞서 제시하였다. 개인정보를 제공하는 기업이 제공받는 기업의 정보보호 수준을 판단하여 고객의 정확한 동의를 기반으로 자율적으로 관리・감독 여부를 선택할 수 있는 환경을 만들어가야 할 것이다.

핀테크 기업에 모든 책임을 부과하거나, 고객의 동의만을 전제로 핀테크 시장을 활성화한다는 것은 정보보호 산업의 특성과는 이율배반적인 면이 있다. 정보보호 규제 개선을 통해 핀테크 산업의 창의성을 살리고 실질적인 자율보안 환경이 정착될 수 있게 모두가 노력하길 제안해 본다.

5.1 한계 및 발전 방향

본 연구에서는 핀테크 기업들의 정보보호 수준을 실제로 측정해 보았다는 데 그 의의가 있으나, 특정 금융기관의 서비스를 이용하는 기업으로 대상이 한정되었다는 점과 간소화된 체크리스트를 통해 실태조사를 해보았다는 것에는 한계점이 존재한다. 향후 연구에서는 다양한 산업군의 소상공인 등 소규모 기업들의 정보보호 실태조사를 실시하여 보다 세부적인 정책 개정 방안에 대한 검토가 필요해 보인다.

References

[1] Financial services commission, “Project assignment task for financial reform-Clear reference criteria for consignment of personal credit information processing,” 2015.

[2] Financial services commission, Financial supervisory service, Ministry of the Interior, “Guidelines for personal information protection in financial field,” pp. 30-33, 2016.

[3] Judgement of Seoul Central District Court, 2008-Ga-Hap-49696, 2011.

[4] Judgement of supreme court, 2011-do-1960, 2011.

[5] Judgement of supreme court, 2016-do-13263, 2017.

[6] Judgement of supreme court, 2016-do-13263, p. 17, 2017.

[7] Kang, M.-S. and Back, S. J., “A Study of Self-Checklist for Personal Information Protection of FinTech Service: For the Simple Payment Service,” The Journal of Society for e-Business Studies, Vol. 20, No. 4, pp. 77-102, 2015.

[8] Kang, T.-H., “A Study on Consigned Party Management System Enhancement for

Personal Information Protection," Journal of The Korea Institute of Information Security and Cryptology(JKIISC), Vol. 23, No. 4, pp. 781-797, 2013.

[9] Kim, G.-Y., "Correct understanding of the differences between consignment of personal information processing and provision of personal information processing to a third-party, http://www.sgsecurity.co.kr, 2016.

[10] Ko, Y.-D., "A Proposal of Enhanced Personal Information Security management Framework of Consigning of Personal Information," Journal of The Korea Institute of Information Security and Cryptology(JKIISC), Vol. 25, No. 2, pp. 383-393, 2015.

[11] Korea communications commission, KISA, "Manual on privacy protection statement for information service providers," pp. 44-48, 2012.

[12] Korea Internet and Security Agency, "Examples of personal information protection counseling," p. 21, 2017.

[13] Korea Internet and Security Agency, "Perspective trend and prospect of fintech Industry in domestic and foreign countries," p. 5, 2015.

[14] Korea Software Industry Association, "Investigation on employees of fintech industrial workforce and training on education," p. 25, 2016.

[15] Ministry of the Interior, "Manual of PERSONAL INFORMATION PROTECTION ACT and related regulations," pp. 90-91, 2016.

[16] Ministry of the Interior, Personal Information Protection Commission, "2016 Survey report on personal information protection," pp. 43-44, 2016.

[17] Ministry of the Interior, Personal Information Protection Commission, "2016 Survey report on personal information protection," pp. 82-83, 2016.

[18] Mun, K.-T., "A Study on the Supply of Personal Information to a Third Person and the Consignment of Personal Information to a Third Person," Ewha Law Journal, Vol. 14, No. 1, pp. 231-252, 2009.

[19] The bank of Korea, "The future of digital innovation and financial services," pp. 50-51, 2017.

저 자 소 개

김조은 (E-mail: joeny@korea.ac.kr)
2016년~현재 고려대학교 정보보호대학원 금융보안학과 석사과정
관심분야 정보보호 컴플라이언스, 개인정보보호 관리체계

김인석 (E-mail: iskim11@korea.ac.kr)
2008년 고려대학교 정보경영공학과 (박사)
2009년~현재 고려대학교 정보보호대학원 교수
FDS산업포럼 회장, 한국정보보호학회 운영위원
관심분야 전자금융보안, 금융 IT 컴플라이언스, 핀테크