전자금융서비스 접근매체 변화에 따른 법제도 개선방안

한세진*

요 약

핀테크의 발전과 금융규제 완화로 금융권의 기술혁신이 활발해지고 있으나, 금융회사들은 전문성 확보와 적기 비즈니스 진출을 위해 기술의 자체육성보다는 전문기관 위탁을 택하고 있어 위탁 리스크가 점점 더 커지고 있다. 특히 핀테크 적용이 활발한 분야가 인터넷뱅킹과 전자결제 분야의 접근매체인데, 예컨대 과거 계좌번호와 비밀번호, 공인인증서로 고정적으로 이루어져 왔던 전자금융의 접근매체가 최근 규제완화로 간편결제, 무매체거래, 바이오인증 등 고도의 전문기술로 다변화되면서 업체 의존도가 높아지는 문제는, 규제당국의 감독대상인 금융회사의 리스크관리 기능과 법령준수 기능이 제3자로 이전됨을 의미하며 이는 곧 금융서비스 위험을 담보하기가 점점 더 어렵게 됨을 시사한다. 특히 접근매체와 같은 본질적 업무의 위탁은 금융회사의 기술 노하우 축적을 어렵게 하여 기술 주도권의 지속적 금융권 이탈을 가속화할 수 있어 대책마련이 필요하다. 본 논문에서는 전자금융거래의 신뢰의 핵심요소인 접근매체의 IT융합에 따른 리스크를 분석하여 이용자보호와 금융서비스 신뢰도 제고를 위한 바람직한 법제 개편 방안을 제시하고자 한다.

A Study on improvement for a means of access to electronic financial service

Han Se Jin*

ABSTRACT

As financial deregulation policies implemented by the government, electronic financial service is improved but security concerns are increasing and ultimately weaken trust in the financial service. Electronic financial service becomes more and more dependant on the IT platform and the initiatives of access device is also gradually shift to that platform. As biometric sensor is mounted on the smartphone, structural change in the access device is coming. It must be a positive signs in terms of fintech development, in the other side, it can cause many problems such as weakness of regulation and ambiguity of principals of responsibility. So in this paper, by analysing this problem-the shift of service initiative-on the access device I'll propose the best way to the the legal amendments.

Key words : 접근매체, 위탁, FIDO, 바이오인증, 보안, 핀테크, 전자금융거래법

접수일(2015년 8월 30일), 수정일(1차: 2015년 9월 11일, 2차: 2015년 9월 18일), 게재확정일(2015년 9월 18일)

* 금융감독원 선임조사역

1. 서 론

본 연구는 기존 금융권 주도의 접근매체가 비금융기관의 참여로 구조적인 변화가 진행되는 가운데 제기되고 있는 안전성과 법제도적 문제점을 살펴보고 개선방안을 제안하고자 수행되었다.

전통적으로 접근매체는 금융기관이 주도가 되어 발급·관리하는 형태이었으나, 정보통신이 발전하면서 플랫폼이 점차 IT산업군으로 통합되고 통제권한 마저도 금융회사를 이탈하는 현상이 발생하고 있다. 접근매체의 주도권 이탈은 전자금융거래법에 명시된 접근매체 발급관리상 금융회사의 의무와 책임과 관련한 많은 문제를 야기시킨다. 예컨대, 접근매체 발급시 금융실명법에 본인확인, 접근매체 플랫폼에 대한 모니터링, 접근매체 위변조에 대한 이용자 보호책임 등이 문제된다. 전자금융의 발전을 도모하기 위해서는 접근매체에 비금융기관의 참여 확대에 따른 안전성 담보의 문제를 해결해야 한다. 본 연구에서는 접근매체의 안전성 확보를 위한 바람직한 법제도 개선방안을 제안하고자 한다. 주요 분석 대상 법은 전자금융거래법이며 접근매체 정의·발급·관리에 대한 기존 법제도의 문제점과 개선방향을 다루고자 한다. 기본 골격은 접근매체 관리·보안 의무를 설명하는 '접근매체 개관', 역대 접근매체 변천 과정을 설명한 '접근매체 변천 과정 및 시사점', 접근매체의 금융회사 주도권 이탈 문제와 개선방향을 다룬 '접근매체 문제점 및 개선방향'으로 구성된다.

2. 접근매체 개관

2.1 접근매체 정의

접근매체란 전자금융거래에 있어서 거래지시를 하거나 이용자 및 거래내용의 진실성과 정확성을 확보하기 위하여 사용되는 수단으로서 전자식 카드 및 이에 준하는 전자적 정보, 인증서 또는 이를 사용하는데 필요한 비밀번호, 금융회사에 등록된 이용자번호, 바이오정보를 말한다(법 제2조 제10호)

2.2. 금융회사의 의무와 책임

접근매체는 금융회사가 본인임을 확인한 후에 발급하여야 하며 선량한 관리자의 주의로써 이용자의 신원 및 권한을 확인해야 한다. 금융회사는 접근매체의 위변조로부터의 안전성을 유지하기 위해 주기적으로 취약점을 분석·평가해야 하며(법 제21조의 3), 외부주문 시 위변조 및 정보유출에 대비한 보안대책을 수립해야 한다(법 제60조). 접근매체의 위변조로 발생한 사고로 인하여 이용자에게 손해가 발생한 경우 금융회사는 그 손해를 배상할 책임을 부담해야 한다(법 제9조). 한편, 접근매체의 분실이나 도난 등의 통지 시점 이전까지는 이용자의 책임이므로 이용자도 관리책임을 피할 수는 없다(법 제10조).

2.3 접근매체 금지 사항

접근매체는 관리·보안에 소홀할 경우 금융사고와 함께 곧바로 재산손실로 이어질 수 있으므로 법 제정 당시(2006년)부터 부정사용과 이와 관련된 범죄를 처벌하기 위한 근거규정을 두고 있다. 양도·양수, 댓가성 또는 범죄 목적으로 대여·보관·전달·유통하는 행위가 금지되며(법 제6조), 위변조 또는 분실·도난된 접근매체를 판매알선·판매·수출 또는 수입하거나 사용, 해킹 등으로 접근매체를 획득하거나 획득한 접근매체를 이용하여 전자금융거래를 한 자, 강제로 빼앗거나, 횡령하거나, 사람을 속이거나 공갈하여 획득한 접근매체를 판매알선·판매·수출 또는 수입하거나 사용한 자에 대해서 7년 이하의 징역 또는 5천만원 이하의 벌금에 처하도록 벌칙을 정하고 있다(법 제49조).

2.4 접근매체에 대한 해외법률 및 관련 연구

미국의 경우 「전자자금이체법(Electronic Fund Transfer Act)」와 「Regulation E」 에서 접근매체(means of access)를 전자금융거래를 개시하기 위해 사용되는 카드나 코드 또는 그 밖의 이용자의 계정에 접근할 수 있는 수단으로 정의하고 있다. 동 법률에 따르면 금융회사는 무권한 거래에 대하여 입증책임을 부담하며(15 U.S.C. 1693g(b)), 이용자는 무권한 거래의 내역서를 최초로 수신한 이후 60영업일 이내에 금

융회사에 이 같은 사실을 알렸다면, 무권한 거래로 인하여 발생된 피해에 대해서 책임을 부담하지 않는다. 하지만 예외적으로 60영업일이 지나서 금융회사에 알린 경우에는 이용자는 피해의 전부를 책임져야 한다. 접근매체가 도난 또는 분실된 경우에는 이용자가 도난 또는 분실된 사실을 인지한 후 2영업일 이내에 금융회사에 통지한 경우 이용자는 피해액의 최대 50달러까지만 책임을 부담한다. 그리고 도난 또는 분실된 사실을 인지한 후 3영업일부터 60영업일 이내의 경우 최대 500달러까지 책임을 부담한다. 60영업일 이후 부터는 이용자가 금융회사에 도난 또는 분실 사실을 통지하기 이전에 발생된 피해 전부에 대한 책임을 부담한다(15 U.S.C. 1693g(a))[2].

유럽연합(European Union)은 유럽경제지역에 2007년 11월부터 「지급결제서비스지침」을 시행하고 있다. 전자금융사고와 관련하여 이용자는 접근매체의 도난 또는 분실, 부당이용 등을 인지한 경우 지급결제서비스 제공자에게 13개월 내에 이 같은 사실을 통지하여야 하며, 만약 통지를 하지 않을 경우 전자금융사고로 인한 피해에 대하여 최대 150유로의 책임을 부담하게 된다. 그리고 이용자의 사기, 고의 또는 중과실 등이 인정되면 지급결제서비스 제공자는 책임을 면하게 된다. 하지만, 접근매체의 도난 또는 분실, 부당이용 등으로 인해 발생된 피해에 대해서는 책임이 감경될 수도 있다. 그 외에 지급결제서비스 제공자는 이용자가 통지할 수 있도록 적절한 방법을 제공해야 하며, 18개월 간 통지사실을 확인시켜줄 수 있어야 한다[2].

그 밖의 영국, 독일, 호주 등 주요국들은 비록 통지기간이 다르지만, 이용자에게 통지의무를 부과하고 있으며, 통지시점에 따라 이용자의 책임이 전부 부담, 감경, 면제 등으로 나뉜다[2]. 국내법률은 해외 법률과 마찬가지로 접근매체 정의와 유사한 내용을 두고 있지만 접근매체 유형과 관리 기준, 처벌대상에 대한 독자적인 규정을 포함하고 있다는 차이가 있다.

관련 연구로서, “접근매체의 양도제한은 위헌인가?(손진화)”에서는 접근매체의 양도를 금지한 전자금융거래법이 개인의 자유와 재산권을 침해하는가에 대하여 ‘위헌이 아니다’ 라는 헌법재판소의 판례를 중심으로 접근매체에 대한 개인의 관리상 주의의무를 강조하고 있다[1]. 그 논거로서 접근매체는 사법상 경제적 가치를 지니고 있기 때문에 이와 달리 자유롭게 통용되어야 할 사회적·경제적 필요가 있는 전자화폐 또는 선불전자지급수단과는 차별화 되며, 따라서 개인의 의사에 따른 자유로운 양도가 금지된다고 하였다. 필자는 이와 같은 접근매체에 대한 원칙과 헌재 판결 근거로 본 접근매체의 사회·경제적 가치를 토대로 하여, 이용자뿐만 아니라 금융회사도 접근매체에 대한 발급·관리업무를 제3자에게 위임하는데 따른 리스크를 같은 맥락에서 논하고자 한다.

“전자자금이체에 관한 연구(이창운)”에서는 접근매체의 도난, 분실, 사고로 인한 피해에 대하여 현행 이용자의 부분적 책임을 규정한 법조항(법 제10조)에 대하여 그 증명책임을 이용자와 금융회사에게 합리적으로 나누어 부담시킬 것을 제안하였다. 이에 대한 논거로서 금융회사가 접근매체 관리·보안에 소홀할 경우 금융사고와 함께 곧바로 이용자의 재산손실로 이어질 수 있으므로 금융회사는 발급·관리의 책임에서 벗어날 수 없다고 강조한다[4].

3. 접근매체 변천과정 및 시사점

접근매체는 본인인증수단과 거래지시수단으로 정의된다. 본인인증수단의 경우, 전통적인 은행거래에서는 종이통장과 인감도장이 사용되었으나, CD/ATM 도입되면서 전자적 카드와 비밀번호로 전환되고, 2000년대 초반 인터넷뱅킹이 도입되면서부터는 거래부인방지를 위해 공인인증서와 일회용 비밀번호가 사용된다. 최근에는 증가하는 인터넷뱅킹 보안사고를 방지하기 위해 고액거래에 전화인증을 적용하는 등 멀티인증이 일반화되고 있다. 거래지시수단의 경우, 최근에는 인터넷전문은행의 도입으로 물리적 계좌개설을 하지 않고도 기존 계좌를 연계한 가상계좌가 도입되고 있는 등 과거 종이통장이나 플라스틱 카드가 점차적으로 사라지고 계좌정보가 없이도 본인확인만으로 거래가 이루어지는 무매체 거래가 활성화되고 있다.

<표 5> 은행분야 접근매체 변화

도입년도	거래채널	거래지시 수단	본인인증 매체
1980년대	CD/ATM, 텔레뱅킹	현금카드	비밀번호
2000년	인터넷뱅킹	전자적 계좌정보	공인인증서, 일회용비밀번호, 추가인증
2010년	모바일 뱅킹		
2015년	인터넷전문은행	무매체	바이오인증 등

한편, 지급결제 분야의 접근매체의 경우, 종전에는 신용카드와 비밀번호가 사용되었으나, 전자상거래의 발전으로 인터넷안전결제(ISP)인증서 또는 안심클릭 비밀번호가 쓰이고 있다. 최근 인터넷 부정결제가 증가하자 고액거래 시 공인인증서가 도입되었고, 2014년부터는 별도의 본인확인 없이 결제비밀번호만으로 결제가 가능한 간편결제가 도입되었다. 간편결제에서는 공인인증서나 전화인증 등 본인인증 수단을 생략하고 결제비밀번호, 안전패턴, 그래픽 인증, 바이오인증 등 단일 접근매체를 사용하는 것이 특징이다[5].

<표 6> 지급결제분야 접근매체 변화

도입년도	결제 방식	거래지시수단	본인인증수단
2003년	인터넷안전결제	카드번호, 카드비밀번호, 유효기간	인증서, ISP비밀번호
2004년	안심클릭		안심클릭비밀번호
2012년	USIM카드		전화인증, 결제 비밀번호
2012년	앱 카드		
2014년	간편결제		

4. 접근매체 문제점 및 개선 방향

4.1 정의조항 개선

시대가 변하고 전자금융 환경이 급격히 변하면서 접근매체를 한정적·열거적으로 정의하는 현행 법률은 금융실무와 많은 차이를 보이고 있다. 첫째, 법률에서 다양한 신규 접근매체의 포섭이 어렵다. 둘째, 정의조항에 특정 인증기술을 명시하고 있는 문제가 있다. 셋째, 유형의 포괄적 정의로 인하여 해석이 모호한 문제가 있다. 예컨대, 접근매체에 '금융회사에 등록된 이용자번호'라고 명시한 부분은 법률에서 의도하지 않은 주민등록번호도 포함할 수 있는 위험이 있다. 따라서 현재의 한정적·열거적 정의를 개념적·포괄적 정의로 전환함이 필요하다.

4.2 접근매체 발급·관리 체계 개선

필자는 그동안 전자금융감독 업무를 하면서 금융회사의 핀테크 서비스에 대한 보안성심의를 수행하면서 핀테크의 발전과 금융규제 완화로 금융권의 기술혁신은 활발해지고 있으나, 금융회사들은 전문성 확보와 적기 비즈니스 진출을 위해 기술의 자체육성보다는 전문기관 위탁을 택하고 있어 위탁 리스크는 점점 더 커지고 있다는 점을 주목하고 있다. 특히 핀테크 적용이 활발한 분야가 인터넷뱅킹과 전자결제 분야의 접근매체인데, 최근 최첨단 바이오인증 등과 결합한 본인인증 수단이 나타나면서 본질적 업무에 해당되는 접근매체 발급·검증 업무를 전문업체에 의존하는 사례를 포함해 이러한 주세가 강해지고 있다. 이와 같은 현상은 규제당국의 감독대상인 금융회사의 리스크관리 기능과 법령준수 기능이 비금융권으로 이전됨을 의미하며 이는 곧 금융서비스 위험을 점점 더 담보하기 어렵게 됨을 시사한다. 특히 본질적 업무의 위탁은 금융회사의 기술 노하우 축적을 어렵게 하여 기술 주도권의 지속적 약화를 불러올 것이므로 문제의 심각성이 크다고 할 수 있다. 일례로, 최근 시장에 출시되고 있는 삼성페이와 같은 신규 전자금융서비스는 고도의 바이오인증기술과 보안이 강화된 마그네틱 비접촉식 방식을 적용한 대중적 인지도가 높은 결제서비스이나, 접근매체의 주도권이 금융회사가 아닌 민간영역이라는 점이 문제가 될 수 있다. 즉 사설 TTP (Trusted Third Party)에 기반한 인증구조상 문제[3], 바이오인증정보 발급·검증 주체가 휴대폰 제조사인 점, 클라우드컴퓨팅 사업자로의 재위탁 구조에 따른 보안 문제를 내포하고 있다. 이와같은 접근매체 주도권이탈에 따른 보안리스크를 해결하기 위해 제안하는 바는, 금융회사의 접근매체 주도권 확보이다. 즉, 접근매체 발급·검증의 위탁을 제한하여 금융회사 주도성을 확보하고, 그 밖의 업무위탁에 대해서

는 금융당국의 심의·의결을 거친 표준계약서를 적용하며, 이를 전자금융거래법에 명시하는 것이다.

4.3 바이오정보 처리 원칙 마련

바이오정보란 개인의 신체 일부분에 대한 특징정보로서 시간이 지나도 변하지 않는 불변성과 개인을 고유하게 식별할 수 있는 고유성 때문에 차세대 인증방법으로 각광을 받고 있다. 반면 바이오정보가 금융거래 접근매체로 이용될 경우 한번 유출되면 재산과 프라이버시 문제를 심하게 훼손할 수 있는 위험성을 지닌 만큼 전자금융거래시 바이오인증에 대한 안전한 처리기준을 마련할 필요가 있다. 개인정보보호법과 같은 타법률에서 바이오정보를 규정하고 있으나, 이는 일반적인 자연인의 개인정보보호 목적의 입법체계로 구성되어 있어, 동 법이 전자금융의 접근매체를 규율하기는 어렵다[7]. 따라서 전자금융감독규정에 (1)이용자 동의 원칙 (2)원본정보 저장 불가 및 특징정보를 개인정보와 분리저장 (3)특징정보부터 원본정보 복원 및 또 다른 식별정보 재구성 불가 (4)바이오정보의 용도를 접근매체로 한정하며 통제 또는 감시 목적으로 이용 금지 (5)처리 목적 달성시 즉시 파기 조항을 신설할 것을 제안한다.

4.4 본인인증기술 평가 기준 마련

상용화된 단일 본인인증 수단들은 대부분 보안적 한계를 가지고 있으므로 다양한 종류의 인증수단을 복합적으로 사용하는 복합인증이 최근의 추세이다. 다만, 복합인증이 사용자의 불편함과 모든 계층의 이용자를 포섭하기 어렵다는 점 등은 단점이 될 수 있다. 따라서 무작정 인증솔루션을 중첩적으로 사용하는 것보다는 개별 인증의 안전성을 보완할 수 있는 최소한의 중복인증이 바람직 할 것이다. 이를 위해 단일인증기술의 안전성에 대한 평가기준을 다음과 같이 제안한다. 평가기준은 크게 (1)인증기관의 신뢰도, (2)인증기술의 보안성 (3)인증정보 저장매체의 보안성으로 구성된다. 첫째, 인증기관의 신뢰도란, 인증정보를 발급·검증하는 기관의 공신력 및 안전성 등을 말한다. 둘째, 인증기술의 보안성이란 본인확인의 가장 본질적 요소로서, 고유식별성과 부인방지성으로 설명될 수 있다. 셋째, 인증정보 저장매체의 보안성이란 본인확인 증표를 저장하는 메모리 영역의 해킹 위험도를 뜻한다. 위 세가지 요소를 통해 인증방법의 종합적인 안정성을 평가할 수 있다.

<표 7> 접근매체 개선방안 요약

개선방안	기존	변경후
정의변경	한정적·열거적 정의	개념적·포괄적 정의
접근매체 발급 관리체계개선	▪ 위탁 금지 불분명 ▪ 사적 위수탁계약서를 통해 위탁	▪ 위탁 대상에서 제외 ▪ 표준위수탁계약서 적용
바이오정보 처리 원칙 마련	없음	바이오정보 수집, 이용, 파기 등 원칙 수립
본인인증기술 평가기준 마련	없음	인증기관의 신뢰도, 인증기술의 보안성, 저장매체 보안성으로 평가

4.5 제안 방안의 의의

최근에 발생한 간편결제 부정결제 사고 사례를 통해 본 제안의 실효성을 설명하고자 한다. 문제가 된 간편결제는 국내 최초의 바이오인증을 도입한 간편결제로서, 접근매체의 발급, 확인, 관리 기능의 대부분을 전문업체에 위탁하고 결제 승인 등 고유기능만을 금융회사가 수행하는 구조이다. 수탁자는 당해 시스템을 클라우드컴퓨팅 사업자에 재위탁하였기 때문에 금융회사는 이상거래탐지시스템(FDS)을 간편결제에 적용할 수 없었고 수탁자의 금융법규 준수 여부도 담보할 수 없는 상황이 전개되고 있었다. 문제는 재위탁처의 불미스러운 사건으로 인하여 다수의 사용자 접근매체에 오류가 발생하고 금융회사는 이를 인지하지 못한채 결제 승인을 처리하는 과정에서 부정결제가 발생한 것이다. 접근매체의 금융권 주도권 확보는 결제과정에 있어서의 위탁리스크를 관리하기 위한 근본적 해결책이다. 아울러 다양한 신종 접근매체를 법률상 포섭할 수 있는 것이 필요하며, 바이오정보와 같이 현행 법률에 명시되지 않은 접근매체 종류에 대해서는 별도의 관리 기준을 마련하여 수집과 이용 및 파기상에 철저한 관리가 되어야만 접근매체에 따른 금융사고를 방지할 수 있다고 본다.

5. 결 론

접근매체는 앞으로 정보통신기술의 진화와 함께 더욱 고도화되고 다양화될 것으로 예상된다. 안전한 접근매체의 도입을 위해서는 접근매체의 위탁에 따른 리스크를 적절히 관리해야 하며 발급 및 관리체계에 대한 법제도상 보안장치를 마련해야 한다. 본 연구에서는 이에 대한 방안으로 세가지 방안을 제안하였다. 첫째, 금융회사의 접근매체 주도권 확보, 둘째, 시대적 변화에 맞게 접근매체 정의조항을 개념적·포괄적으로 전환, 셋째, 바이오정보에 대한 처리규정 신설, 마지막으로 본인인증 기술 평가기준 마련을 제안하였다.

참고문헌

[1] 손진화, “접근매체의 양도제한은 위헌인가?”, 經營法律, 2012.7월
[2] 금융보안원, “주요국 전자금융사고 책임소재 관련 법규 분석 및 시사점”, Vol.2013-001, 2013.6월
[3] 김수형 · 조영섭 · 최대선, “핀테크 시대: 새로운 인증 기술을 요구하다”, 정보과학회지, 2015.5월
[4] 이창운, “전자자금이체에 관한 연구”, 金融法硏究 제12권 제1호, 2015.4월
[5] 한세진, “전자상거래 지급결제의 핀테크 활성화를 위한 보안 및 법제도적 과제”, 융합보안 논문지, Vol. 15, No.2, 2015.3월
[6] 박정훈, “바이오매트릭스의 이용에 따른 법적 과제”, 慶熙法學 제47권 제4호, 2012.12월

[저 자 소 개]

한 세 진 (Han Se Jin)

2011~현재 : 금융감독원 선임조사역
2001~2011 : KT 통신망연구소 책임연구원
2001년 8월 : 서강대학교 컴퓨터학과 석사
1998년 2월 : 서강대학교 컴퓨터학과 학사

email : hsjhjb@fss.or.kr