새로운 전자금융거래법에서의 전자금융사고 대응 방안에 관한 연구*

조성인** · 박태형*** · 임종인***

요 약

2007년 1월 시행된 전자금융거래법에서는 전자금융거래의 안전성과 금융소비자 보호를 위하여 전자금융사고 발생시 금융회사에 무과실책임을 부여하였다. 그러나 금융범죄자에 의한 무권한 금융거래 또는 금융소비자의 도덕적 해이에 따른 금융거래가 발생하였을 경우, 사고 원인을 파악하거나 금융소비자의 고의·중과실 여부를 판단하기 어려운 정보의 비대칭 현상이 발생한다. 이와 같은 금융사고 위험을 예방 또는 차단하기 위하여 금융거래정보 통보제도의 개선과 금융거래 장소정보를 활용한 IT 컴플라이언스 기능을 강화함으로써 금융소비자를 보호할 수 있는 방안을 제시하고자 한다.

Research about the Financial Institution's Preparations for Electronic Financial Accidents under New e-Financial Transaction Act

Soung In Cho** · Tae Hyoung Park*** · Jong In Lim****

ABSTRACT

By e-Financial Transactions Act enacted in January 2007, the financial institutions are responsible for indemnifying user's damage to ensuring security of the electronic financial transactions and to protecting financial users when suffering from electronic financial accidents. However, when occurring unauthorized financial transactions or electronic financial accidents by user's moral hazard, it is difficult to determine where the accidents happened at and whether caused by the intention or gross negligence of users.

To protecting financial parties and ensuring the security and reliability of electronic financial transactions, this paper attempts to propose the means, what enhance the notification process about financial transactions and to strengthen IT regulatory compliance by using area information about electronic financial transactions, to protect risk of the financial accidents.

Key words : Electronic Financial Transaction, Electronic Financial Accident, Internet Banking Accident, IT Compliance

---

* 이 연구에 참여한 연구자(의 일부)는 '2단계 BK21사업'의 지원비를 받았음.

** 금융감독원

*** 고려대학교 정보경영공학전문대학원

1. 서 론

IT 기술 및 통신기술의 급격한 발전과 금융소비자의 기대수준 향상에 따라 금융업무의 정보화 수준이 향상되었고, 전자금융거래의 활성화에 따라 은행 및 증권업무를 중심으로 전자금융 고객의 지속적인 저변 확대와 전자금융 거래가 확산 발전되고 있으며, 새로운 전자금융거래의 출현에 따른 법률관계를 명확히 하고 전자금융 사고 발생시 금융회사의 무과실책임 부담 원칙과 비금융회사의 전자금융업 진입 기준 및 전자금융업자의 감독 기준의 설정 등을 통하여 금융소비자의 보호 및 전자금융업의 건전한 발전을 위하여 전자금융거래법이 2007년 1월 시행된 바 있다.

2007년 12월말 현재 우리나라의 인터넷 이용률은 76.3%(이용자수 34백만 명, 만 6세 이상 조사대상)를, 컴퓨터 보유율은 80.4%를 차지(2005년말 현재 OECD 국가 중 인터넷 보급률 1위)하였으며, 인터넷 이용자의 57.3%가 인터넷 쇼핑을, 39.1%가 인터넷 뱅킹을 각각 이용하고 있는 것으로 나타났다[1].

이러한 외향적인 발전에 따라 전자상거래 및 전자금융거래의 편의성과 안전성 확보를 위한 참여자의 요구 수준은 높아졌으나, 그에 따른 서비스 제공자의 상대적인 대응은 그렇지 못한 실정이다. 고객의 정보 보호와 안전한 거래 형성을 위한 경영진의 인식 제고, 전문 인력자원 양성 및 정보유출 대응시스템 구축 등에 대한 지속적인 관심과 투자가 요구됨에도 최근 일부 금융회사와 통신회사 등에서 고객정보의 유출 사고가 발생하는 등 고객정보 관리의 취약점이 나타나고 있다. 개인정보의 탈취 유형은 과거 자기 과시형에서 최근에는 경제적 이익 취득 목적으로 변화하고, 사회공학적인 방법으로 고객 재산을 탈취하는 등 전자금융사고는 보다 전문적으로 발전하고 있는 추세이다[2].

전자금융거래법에서는 금융사고가 발생하였을 경우 상대적 약자인 금융소비자를 보호하기 위하여 금융회사에 무과실 책임을 부여하였으나, 금융범죄자에 의한 무권한 금융거래시 금융회사는 금융거래의 원인 파악에 중요한 정보인 전자금융거래의 발생 장소 등 상세정보를 확보할 수 없어 사고원인을 파악하는데 미흡한 환경이며, 금융소비자의 도덕적 해이로 인한 금융사고 발생시 그 원인 분석과 금융소비자의 고의·중과실 또는 경과실 여부를 판단하는데 요구되는 관련된 상세정보를 확보할 수 없어 금융소비자와 금융회사와의 정보 비대칭 현상이 나타나는 등의 문제점이 있다.

전자금융시장에서는 금융소비자, 금융회사 뿐만 아니라 전자결제대행기관, 통신회사 등도 전자금융거래에 참여하여 상호의 목적을 달성하는 금융거래 참여자이다. 따라서 금융사고가 발생하였을 경우에는 당사자 모두가 피해자가 되기 때문에 해커 등 눈에 보이지 않는 공격자로부터 방어하는 것뿐만 아니라, 고객인 금융소비자와 서비스 제공자인 금융회사가 자체적으로 방어할 수 있는 환경 구축이 목적이 되어야 할 것이다.

본 논문은 무권한 금융거래 등 금융사고 위험으로부터 회피하거나 연속적인 금융사고의 발생 및 피해규모를 축소하고 전자금융거래의 투명성을 확보하기 위하여 금융소비자의 금융거래정보 통보제도의 개선과 금융회사의 IT 컴플라이언스 기능을 강화함으로써 금융소비자 보호 및 금융산업의 건전한 발전을 도모하기 위한 효율적인 방안을 제시하고자 한다.

본 논문의 구성은 제 2장에서는 전자금융거래의 사고 현황 및 유형을 분석하고, 제 3장에서는 전자금융거래법 시행에 따른 금융사고 발생시 금융회사의 대응환경 변화에 대한 문제점을 살펴보며, 제 4장에서는 금융소비자 보호를 위한 금융회사의 금융사고 대응방안을 제시하고, 제 5장에서는 결론을 내린다.

2. 전자금융사고 현황 및 유형 분석

2.1 전자금융거래의 발전

우리나라의 전자금융거래는 1980년대 초 각 은

행별 본지점간 온라인 업무로 시작으로 1987년 PC 뱅킹 서비스의 도입과 1989년 타행환 공동망을 기점으로 본격적인 전자금융 서비스를 가동하였고, 1999년 인터넷 뱅킹 시스템의 서비스를 제공하였으며, 증권의 경우 1997년 4월에 온라인증권거래업무를, 보험의 경우 1998년 3월에 인터넷 보험판매 업무를 각각 개시한 바 있다.

금융감독원에 따르면 2007년 말 현재 은행의 전자금융거래 이용자수는 36백만 명(이용건수 : 1,383백만 건)으로 2004년 대비 52.9%(이용건수 : 153.8%) 증가하여 전체 이용건수에 24.7%를 차지하였고, 사이버 증권거래는 5,809조 원으로 전체 증권거래의 60.9%를 차지하였으나, 보험과 신용카드거래는 각각 0.4%, 7.0%를 차지하였다. 또한 개인용 공인인증서 발급건수는 15,881천 건으로 2004년 대비 154.9%가 증가하였다.

〈표 1〉 금융권역별 전자금융 취급실적

(단위 : 천 명, 천 건, 십억 원)

구 분		2004년	2005년	2006년	2007년
은행 (인터넷 거래)	이용자수	23,372	25,108	31,943	35,757
	이용건수	544,839 (13.1%)	1,086,419 (22.5%)	1,125,698 (19.9%)	1,382,827 (24.7%)
	이용금액	3,178,885	4,719,042	6,144,860	8,376,674
증권	거래금액	3,485,616 (57.5%)	4,152,590 (59.5%)	4,817,750 (61.2%)	5,809,270 (60.9%)
보험	이용건수	365 (0.7%)	218 (0.4%)	162 (0.2%)	255 (0.4%)
	이용금액	1,321	750	514	421
카드	이용건수	153,211 (6.2%)	163,424 (6.1%)	213,139 (6.8%)	245,810 (7.0%)
	이용금액	74,652	67,306	68,613	74,672

주) * ( )는 금융권역 전체에서 차지하는 비율임.
출처 : 금융감독원.

은행 및 증권업무에 비하여 보험거래의 전자금융거래 비중이 저조한 이유는 보험상품 종류의 다양성 및 복잡성으로 보험판매원을 통한 대면거래를 주로 이용하였고, 신용카드는 가맹점에서의 직접적인 물품 구입 등으로 전자금융의 비중이 적게 차지한 것으로 분석된다.

2.2 전자금융사고 발생 현황

전자금융업무는 이용자가 금융회사의 점포를 직접 방문하지 않고 인터넷 등 유무선 통신매체를 이용하여 비대면으로 처리하는 업무이며, 전자금융사고는 명시적으로 정의되고 있지 않지만 전자금융거래법 제2조 및 제9조의 규정에서 유추하여 금융회사 등이 전자적 장치를 통하여 제공하는 금융상품 서비스, 거래지시 과정에서 접근매체의 위·변조 또는 해킹이나 전산장애 등 전자적 전송·처리 과정에서 발생한 사고라 할 수 있다[3, 4].

전자금융거래에서의 금융사고는 창구거래의 금융거래에 비하여 그 어느 때보다도 고객정보 보호의 중요성이 강조되고 있는데, 이는 개인 금융정보 유출시 개인정보 또는 신용정보를 이용하여 금융사고 또는 사회적 범죄로 이어질 수 있기 때문이다. 고객정보 유출과 관련된 사고 범위는 은행 등 특정권역에 그치지 않고 보험, 증권, 카드 등 여러 분야에 연계되어 사고가 발행하고, 사이버 금융범죄의 경우와 같이 거래당사자 간에 책임을 규명하기 어려운 쌍방 무과실사고 등의 형태로 다양하게 나타나고 있다.

〈표 2〉 전자금융사고 발생 현황

(단위 : 건, 백만 원)

구 분	2004년	2005년	2006년	2007년
은 행	20(192)	13(411)	2(15)	22(325)
증 권	-	1(0)	-	-
보 험	-	-	-	1(6.5)
카 드	-	-	-	-

출처 : 금융감독원.

전자금융사고는 이용 수단의 변화에 따라 그 대상과 방법도 변화하고 있는데, 1998년 이후 인터넷 뱅킹이 일반화되고 내부직원에 대한 통제가 강화

됨에 따라 전자상거래 결제 등 신종 전자금융업의 출현과 더불어 외부인들에 의한 사고가 증가하기 시작하였다. 이는 개인 PC 등이 갖고 있는 취약점을 이용하여 다양한 해킹 공격 수법이 개발되고 대응체계가 제대로 갖추어지지 않고 범행 장소를 은닉할 수 있는 컴퓨터의 이용이 자유로워지면서 나타난 현상이다.

금융회사는 금융소비자 정보를 보호하고 해킹 등의 침해를 차단하기 위하여 전자금융거래 종류별 안정성 기준을 마련하여 H/W, S/W의 안전한 운영을 위한 시스템을 구축, 운영하고 있으며, 2005. 5월 시중은행의 인터넷 해킹사고 발생 이후 금융당국에서는 "전자금융 보안 종합대책"을 마련하여 개인정보 유출로 인한 전자금융사고의 피해를 최소화하고 안전한 전자금융거래를 위하여 OTP 통합인증센터의 설립 및 금융권 공동 사용을 위한 OTP 통합인증 시스템 구축, 보안카드 정보의 분할 입력 등의 제도를 운영하고 있다[5].

2.3 전자금융사고의 유형 분석

은행권역의 전자금융사고에 관한 일반적인 현상으로 1999년에는 텔레 뱅킹 사고가, 2001년에는 PC뱅킹에 대한 사고가, 2003년부터 2004년까지는 카드 복제사고가, 2005년에는 인터넷 뱅킹의 해킹, 피싱 등 금융사고가 주를 이루었으나, 2005년 금융당국의 관리방안 강화 이후 2006년의 금융사고 건수는 상당히 줄어들었음을 알 수 있다. 그러나 2007년 이후에는 카드 복제와 변형된 해킹, 피싱 사고가 복합적으로 발생하고 있으며, 범죄 연계, 자녀납치 등 이용자의 심리를 이용한 전화사기 사고로 인터넷 금융거래를 이용하여 일반 국민들의 귀중한 금융재산을 절취하고 있다.

이와 같이 금융사고 유형의 변화를 분석해 보면 금융거래에 필요한 개인정보의 습득이 용이한 대상부터 시작하고 있으며, 사고 이후 보호대책이 강화되면 다른 대상으로 변경되는 것을 알 수 있다[2].

〈표 3〉 은행권역의 전자금융사고 내역

(단위 : 건, 백만 원)

구 분		2004년	2005년	2006년	2007년
인터넷 뱅킹	건수	1	5	2	11
	금액	3	149	15	152.6
텔레뱅킹	건수	5	6	-	-
	금액	162	262	-	-
카드위조·복제	건수	6	-	-	11
	금액	26	-	-	172.4
프로그램 오류	건수	8	2	-	-
	금액	1	0	-	-

출처 : 금융감독원.

3. 전자금융거래법 시행에 따른 전자금융사고시 금융회사의 대응 환경 변화

금융회사는 전자금융거래법의 안전성 확보의무 등에 따라 전자금융거래가 안전하게 처리될 수 있도록 선량한 관리자로서의 주의를 다하며, 전자금융거래의 종류별로 전자적 전송이나 처리를 위한 인력, 시설, 전자적 장치 등 정보기술부문 및 전자금융업무에 관한 기준을 준수하기 위하여 내부통제장치를 마련하고, 기술적인 대응체계를 마련하여 운영하고 있다[6].

금융소비자 측면에서는 해킹에 의한 공인인증서, 비밀번호 등 중요매체가 유출되는 1차 사고를 알기 곤란하며, 이에 따른 금전유출의 2차 사고 역시 본인이 금융거래 내역을 확인하기 전에는 인지하기 어렵다. 금융회사 측면에서는 비금융회사가 전자금융거래의 참여자로 개입하면서 전자금융거래의 복잡성이 증가되었고, 전자금융거래의 연속성에 대한 기술적 분절화 현상으로 사고원인을 파악하기 어려운 쌍방 무과실 금융사고, 중요정보의 유출에 따른 무권한 금융거래 개연성, 그리고 금융소비자의 도덕적 해이에 의한 금융사고 등은 금융회사가 즉시 대응하기 어려울 뿐만 아니라 전자금

융거래법의 시행으로 금융회사의 무과실책임 부여 및 입증책임이 가중되고 있다.

3.1 금융회사에 대한 무과실책임 부여

3.1.1 금융회사의 입증 책임에 따른 부담 가중

전자금융거래법의 시행으로 전자금융거래 서비스 제공자의 범위는 금융거래실명법에 의한 금융회사뿐만 아니라 전자금융업자 및 전자금융보조업자로 확대되었고, 전자금융거래 당사자의 의무사항으로 전자금융사고가 발생하여 이용자에게 손해가 발생하였을 경우 금융회사 등에게 무과실책임을 부과하였다. 다만 이용자에게 고의나 중대한 과실이 있는 경우에 한하여 금융회사 등의 책임을 경감할 수 있도록 하는 등 제한적으로 설정하고 있는데, 이는 전자상거래에 따른 원활한 거래대금 지급과 안전성 확보 및 소비자의 편의성을 위한 것으로 보인다[7].

과거에는 전자금융거래기본약관에 의거 금융사고 발생시 입증책임을 금융소비자에게 부과하여 금융거래의 전문성 및 정보 관리능력에 상대적으로 열위에 있던 금융소비자에게는 과다한 부담이었으나, 전자금융거래법에서는 금융회사의 과실이 없더라도 원칙적인 책임을 부담하도록 하였으며, 비금융회사의 결재업무 개입에 따른 기술적 분절화 현상(Technical Segmentation)으로 원인이 불분명한 금융사고가 발생하였을 경우에도 금융회사가 우선 배상하게 하고 구상권을 청구하도록 한 것은 상대적으로 약자의 위치에 있는 금융소비자를 두텁게 보호하기 위한 조치이다[8].

이와 같이 금융기관에 무과실책임을 부여한 이유는 첫째, 인터넷 뱅킹의 해킹 사고와 같이 전자금융거래가 복잡하고 전문적이기 때문에 정보의 비대칭에서의 약자인 이용자가 사고의 원인을 규명하거나 입증하기란 거의 불가능하여 사실상 모든 책임이 이용자에게 전가될 우려가 크다고 보았던 것이고, 둘째, 접근매체의 위변조의 경우 금융기관이 이를 입증하기 어려우므로 금융기관 등에게 과도한 부담이라고 주장하는 견해에 대해서는 접근매체의 관리책임은 금융기관도 함께 분담하고 있는 부분이며 접근매체의 보안성 강화 등 제도적 보완장치의 개발 등도 금융기관이 담당할 부분이라고 하고 있다[9].

그러나 금융사고 원인이 금융회사에 있는 것이 아니고 도덕적 해이 등 금융소비자에게 원인이 있는 경우 금융회사는 이용자의 고의 또는 과실을 입증할 수 있는 상세정보를 알 수 없으며, 비금융회사에 사고 원인이 있는 경우 또는 금융소비자 과실에의한 중요정보가 유출되어 금융범죄자의 무권한 금융거래가 발생한 경우에도 금융회사는 무과실책임을 면하기 어렵기 때문에 상대적 손실을 입을 비대칭성을 내포하고 있다.

3.1.2 금융소비자의 도덕적 해이에 의한 금융사고 대응의 한계

전자금융거래에 있어서 금융소비자는 공인인증서 또는 비밀번호의 유출 등의 사고가 발생하였을 경우에는 지체없이 금융회사에 통보하여 자신의 금융자산에 손실이 없도록 선관주의의무를 다하여야 하나, 현실적으로 해킹 등에 의한 경우 중요정보의 유출 사실을 알기 어려우며, 금융회사는 금융소비자가 악의적으로 전자매체 등 중요정보를 타인에게 양도한 이후 금융사고를 발생시키는 도덕적인 해이가 발생하였을 경우에 금융소비자의 고의 또는 중대한 과실 여부를 판단할 정보를 갖고 있지 못한 실정이다.

이와 같이 금융소비자의 고의 또는 중대한 과실에 대한 입증책임을 금융회사에서 부담하게 됨으로써 금융회사의 책임이 불공평하고 과다하게 커질 우려가 있을 뿐 아니라 전자금융 거래과정에서 자칫 이용자 측의 도덕적 해이를 야기할 수 있는 문제점이 있다[10].

전자금융거래는 대면거래와는 다르게 사이버 공간상에서 거래되므로 금융거래 발생장소 등을 알

수 없으며, 금융소비자(금융거래 지시자)로부터 위탁받은 금융거래를 이행하는 금융회사(금융거래 행위자)는 금융거래의 정당성을 공인인증서, 비밀번호의 확인 등의 방법 이외에는 확인하기 곤란하므로 무권한 금융거래 또는 불법 금융거래를 사전에 알 수 없으며, 도덕적 해이로 인한 부당한 거래 역시 금융거래의 이행을 거부할 수 없으므로 금융회사의 무과실책임 부담에 따른 불평등한 현상이 나타날 수 있다.

3.2 전자금융거래의 참여자 및 복잡성 증가

3.2.1 전자금융사고에 대한 원인 파악의 어려움

기존의 대면 금융거래는 금융소비자가 금융회사 영업점에 내점하여 직원을 통한 창구거래가 중심이 되었으나, 인터넷 금융거래가 활성화되어 결제중계업무가 통신 네트워크를 활용하여 이루어짐으로써 금융소비자에게 다양성과 편리성을 제공하고 있다. 그러나 통신사고 또는 제 3자의 금융사고에 대한 결제처리 정보의 전달이 원활하지 못할 경우에는 금융소비자와 금융회사 및 비금융회사 사이에 책임 범위가 모호해지고 금융거래의 신뢰성이 하락할 우려가 있다.

이러한 현상은 금융거래 당사자인 금융소비자와 금융회사 이외에 전자금융보조업자와 통신회사 등이 결제중계업무에 참여하거나, 거래비용을 통신비용으로 결제하는 등 통신기술을 보유하고 있는 비금융회사가 결제중계업무를 대행하고 있기 때문이다.

이와 같은 기술적 분절화 현상이 지나치게 진행되고 서비스 전달 채널이 복잡해질수록 금융 서비스를 제공하는 비금융회사의 적격성 문제, 거래의 신뢰성 문제와 금융소비자의 이익 침해 가능성이 커질 수 있으며, 고객의 중요정보를 고유 업무의 확장을 위한 금융거래 이외의 방법으로 활용하는 등 부정적한 활용 사례가 나타나고 있다.

전자금융거래는 기본적으로 IT 기반하에 운영되며 금융회사나 금융소비자 모두가 이용자의 입장으로 볼 수 있으므로 양쪽 모두 귀책사유가 없는 IT 관련 사고가 발생할 수 있는 단초를 제공한다. 양측 모두 충분한 노력을 기한다 하더라도 모든 IT 문제를 완전히 통제하는 것은 불가능하기 때문에 쌍방 무과실 사고가 발생할 수 있을 것이며, 금융사고 예방을 위하여 금융회사 또는 이용자가 직접 자신의 컴퓨터 운영체제에 취약점을 보완하고 인터넷에 등장하는 최신의 해킹기술이나 바이러스에 항상 최상의 대응을 한다는 것은 사실상 불가능하다[8].

또한, 전산시스템의 오작동, 금융회사 또는 이용자의 부주의, 해킹, 피싱 등 제 3자 개입 등에 의한 금융사고의 발생경로는 다양하기 때문에 전자금융사고가 발생하였을 경우, 해당 사고가 어떤 경로에 의해서 발생하였는지 정확히 알기는 쉽지 않다. 이와 같이 정확한 정보 확인이 곤란한 영역이 존재하기 때문에 원인식별의 문제(Identification Problem)[11]가 발생하고, 정보의 비대칭성 및 원인식별의 문제는 전자금융사고에 대한 책임 귀속을 결정하는데 있어서 어려움을 초래하고 있다.

3.2.2 금융소비자의 중요정보 유출에 관한 인지 곤란

전자금융거래법의 시행에 따라 금융소비자가 접근매체의 분실 또는 도난시 책임범위에 대하여 금융회사는 이용자로부터 접근매체의 분실·도난 통지를 받은 때에는 그 때부터 제 3자의 사용으로 발생한 손해에 대하여 책임을 지도록 하였다. 그러나 금융소비자는 신용카드 또는 전자매체(비밀번호, 공인인증서 등)의 유출, 분실 또는 제 3자에 의한 금융자산의 탈취 등 금융사고가 발생하였을 경우에는 지체없이 금융회사에 통보하여 자신의 금융자산에 손실이 없도록 대응하여야 하나, 해킹 또는 도난에 의한 중요정보가 유출되는 1차 사고와 이에 따른 무권한 전자금융거래의 2차 사고는 동일한 방식을 이용하여 계속 반복될 수 있는 심각성이 있다[12].

그리고 무권한 금융거래를 막기 위한 기술 개발에 비례하여 이를 악용하려는 기술, 또한 개발 발전된다고 보아야 하므로 근절하기 어렵고, 이러한 무권한 금융거래가 발생할 경우 쌍방 무과실책임으로 누가 손해를 부담하여야 하는지 문제가 발생하며, 즉시적인 본인 인지가 어려워 금융거래정보 확인 등 일정한 시일이 지난 이후에 사후적인 인지가 될 수밖에 없다.

대면거래인 신용카드의 경우 가맹점은 본인의 정당성 확인을 위하여 서명 확인과 일정금액(50만원)이 넘는 경우 신분증 확인 절차를 거치며 아울러 위험거래를 인지할 수 있는 전산시스템을 운영하고 있는 반면, 비대면거래인 전자금융거래는 사용자 ID, 비밀번호, 공인인증서 등으로 본인 정당성 여부를 확인하고 있어 사고 예방에 상대적으로 미흡한 환경이다.

전자금융거래의 비대면, 비서면 거래방식에 대한 특수성과 공간적 금융거래 자율성으로 인하여 금융회사는 고객의 금융거래에 대한 장소 등을 확인할 수 없는 등 상세정보를 관리하고 있지 못하므로 금융소비자의 정당한 금융거래 여부를 파악할 수 있는 위험거래인지 시스템을 운영하기 곤란하다. 또한, 금융소비자 역시 중요 접근매체의 분실 여부와 발생 시점을 알기 어려울 뿐만 아니라 이에 따른 금융자산의 변경 사실도 즉시적으로는 알 수 없으므로 위험관리에 취약하다.

4. 금융소비자 보호를 위한 금융회사의 전자금융사고 대응방안

금융소비자는 해킹에 의한 중요정보의 유출 및 무권한 금융거래의 개연성 등 금융사고 발생 위험을 축소하기 위하여 공인인증서, 비밀번호 등 중요정보의 유출 방지를 위하여 철저히 관리하여야 한다. 금융회사 무과실책임 부담에 따른 금융소비자의 도덕적 해이에 의한 금융사고의 발생 등은 금융거래의 신뢰성 및 안정성을 저해할 수 있는 요인이 되는 바, 이로 인하여 금융소비자 보호 및 금융거래 발전에 역행하는 현상으로 나타날 수 있으므로, 이러한 전자금융거래의 역기능에 대한 대응 방안으로 다음과 같이 금융회사가 관리하고 있는 금융거래정보의 활용 방안을 모색하는 등 전자금융거래 사고 예방을 위한 IT 컴플라이언스 기능 강화를 통한 시스템적 관리방법 개선 방안을 제시하고자 한다.

4.1 금융거래정보를 활용한 IT 컴플라이언스 기능 강화

4.1.1 전자금융거래의 위험거래인지 시스템 운영

금융회사는 전자금융거래법에 의거 전자금융거래내역을 확인할 수 있도록 필수 기록항목을 정하여 관리하고 있는데, 인터넷 뱅킹의 경우 금융거래 이용자 ID, 거래일시, 계좌번호, IP 정보 등을 관리하고 있다. 그러나 정보통신망법에서는 통신회사가 IP와 관련된 상세정보 등을 제공하는 것에 대하여 개인정보 보호를 목적으로 당사자 이외의 자에게 중요정보의 수집 및 이용을 제한하고 있다. 이에 따라 금융회사는 현재 IP 정보 자체만은 이용할 수 있으나 금융거래 장소 정보의 특성을 거의 활용할 수 없는 실정이다.

인터넷을 이용하는 비대면 전자금융거래는 본인의 정당성 확인방법을 창구거래 또는 신용카드의 대면거래와 다르게 공인인증서, 비밀번호, 보안카드 등을 통하여 확인하고 있다. 그러나 해킹 등의 방법으로 중요정보를 탈취하거나 도덕적 해이에 의한 전자금융사고의 경우에는 본인의 진정성 확인에 한계가 있을 수 밖에 없으며, 이로 인하여 금융회사는 손해배상 책임으로부터 피할 수 없을 것이다.

이에 반하여 신용카드회사는 신용카드를 통한 불법거래를 차단하기 위하여 금융거래 발생장소인 가맹점의 위치정보 또는 금융거래의 발생 시간차 등의 정보를 활용하는 위험거래인지 시스템을 구축하여 운영함으로써 금융소비자를 보호하고 있다.

〈표 4〉 금융창구, 신용카드 및 전자금융의 거래행태 비교

구 분	창구거래	신용카드거래	전자금융거래
근거법규	금융실명법, 은행법 등	여신전문 금융업법	전자금융거래법, 전자서명법 등
거래행태	대 면	대 면	비대면
정당성 확인	창구 직원 (신분증 등)	가맹점 직원 (카드 보유, 신분증 등)	전산시스템 (공인인증서 등)
거래장소	지점 정보	가맹점 정보	-
위험관리	관리 가능	관리 가능	-

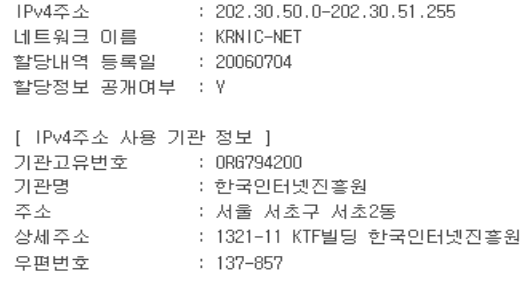
그러므로 전자금융거래의 비대면, 비서면 특수성에 비추어 전자금융의 무권한 거래, 위험거래 등 불법 거래로부터 금융사고를 예방하기 위하여 금융회사는 금융거래 이용자의 IP 정보를 금융거래 장소정보로 활용하는 위험거래인지 시스템을 구축함으로써 금융소비자를 보호하는 것이 효율적이라고 판단된다.

개인의 중요 정보의 오·남용에 대한 프라이버시는 응당 보호받아야 하겠지만 금융자산 관리의 중요성에 대한 효익이 더욱 클 수 있다면 금융소비자의 금융자산의 안전성 및 비대면거래 형식의 전자금융거래 특수성을 감안하여 예외적으로 일부 규제를 완화할 필요가 있으며, 과도한 개인정보 보호에 대한 역효과를 극복하여 금융사고의 사전 예방 또는 건전한 금융거래를 보호할 수 있는 기반 형성이 될 것이다.

아울러 위험거래인지 시스템에 금융소비자의 전자금융 거래간의 시간 차이, 금액 규모, 상거래업자 사업영역, 사용 장소 등 금융거래 행태를 분석하여 위험거래 여부를 판단할 수 있도록 체계화함으로써 금융소비자를 보호하는데 중요한 기반이 될 수 있다고 기대한다.

4.1.2 IP 정보를 활용한 해외로부터의 위험거래 대응

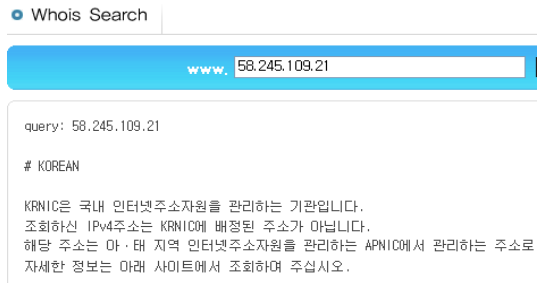
국내에서 사용되고 있는 IP 정보는 집중관리기관인 한국인터넷진흥원에서 관리하고 있으며, 전자금융 거래시 발생되는 이용자 IP 정보는 금융회사에서 관리하고 있다. 위에서 언급한 바와 같이 전자금융거래의 역기능을 극복하기 위하여 국내 등록된 IP 정보 및 이와 관련된 장소정보를 집중관리기관으로부터 전달받아 금융거래 장소정보로 활용할 수 있으면 무권한거래, 위험거래 등 불법거래를 예방하는데 상당한 효과가 있을 것으로 판단된다.


IPv4주소 : 202.30.50.0-202.30.51.255
네트워크 이름 : KRNIC-NET
할당내역 등록일 : 20060704
할당정보 공개여부 : Y

[IPv4주소 사용 기관 정보]
기관고유번호 : ORG794200
기관명 : 한국인터넷진흥원
주소 : 서울 서초구 서초2동
상세주소 : 1321-11 KTF빌딩 한국인터넷진흥원
우편번호 : 137-857

(그림 1) 국내 IP 주소 인터넷 주소 제공 화면 (www.whois.nida.or.kr)

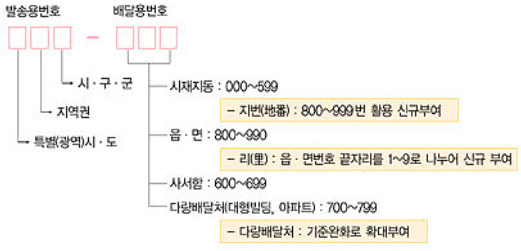
해외에서 전자상거래의 결제자금 이체 또는 전자금융거래를 시도하는 경우, 금융회사는 이용자의 IP 주소를 집중관리기관의 IP 종합정보와 비교하여 해당 IP 주소의 발신지가 국내 또는 해외임을 알 수 있다. (그림 2)와 같이 중국 소재의 IP(예 : 58.245.109.21)에서 시도한 금융거래의 경우 사전에 차단하거나 또는 금융예금자의 확인을 통하여 위험거래를 회피할 수 있을 것이다.



(그림 2) 해외(중국) IP 주소 조회시 화면

4.1.3 IP 정보와 우편번호 지역정보를 활용한 위험거래 대응

인터넷을 이용하기 위하여 IP 주소 또는 도메인을 신청하는 경우, 신청자는 ISP(인터넷 서비스 관리자)에게 기관(상호)명, 주소, 우편번호 등을 제공하고 있으므로 IP 주소와 우편번호를 연결시켜 인터넷을 통한 금융거래 또는 전자상거래 장소정보를 파악할 수 있다.



(그림 3) 우편번호 관리 체계도

(그림 3)을 통하여 알 수 있듯이 우편번호 관리체계는 행정단위로 구분하여 관리하고 있으므로, 금융거래 장소가 통상적으로 일정시간 내에 원거리에서 발생한다면 위험거래로 판단하여 금융소비자에게 거래 정보를 확인하거나 또는 거래를 중지함으로써 위험거래를 예방할 수 있을 것이다.

전자금융거래시 IP 정보와 우편번호 정보를 접목하면 거래지역을 구분할 수 있는데, 서울지역 우편번호의 앞부분 1자리는 “1xx”이고 부산지역 우편번호의 앞부분 1자리는 “6xx”이므로 우편번호 앞부분 3자리를 모두 활용하면 금융거래 발생장소에 대한 시군구 지역정보를 파악할 수 있으므로 일정시간내 원거리에서 발생하는지 여부 또는 금융소비자가 평소에 거래하지 않는 지역 여부 등을 알 수 있으므로 위험거래 여부를 판단하는데 중요한 정보로 활용할 수 있을 것이다.

이와 같이 위험거래인지 시스템의 활용은 전자금융거래의 유형을 분석하여 무권한 금융거래 등 위험 또는 불법 금융거래를 사전에 예방 또는 추가 금융사고를 차단하는데 중요한 역할을 할 것으로 생각하며, 안전한 금융거래를 형성하는데 중요한 기반이 될 수 있을 것이다.

4.2 금융거래의 투명성 확보를 위한 금융거래정보 통보제도 개선

금융사고가 발생하였을 경우 전자금융거래의 참여자의 증가로 인한 기술적 분절화 현상 및 원인식별의 문제 등으로 인하여 사고 발생에 관한 명확한 원인 확인이 곤란한 영역이 발생하여 책임 귀속을 결정하기 어려워 쌍방 무과실책임이 나타날 수 있다. 무권한 금융거래 또는 금융소비자의 도덕적 해이에 의한 금융사고의 경우는 금융회사의 정보 비대칭현상이 발생하여 과실 책임자가 존재함에도 불구하고 금융회사는 무과실책임을 회피할 수 없는 실정이다.

〈표 5〉 금융권역별 SMS 이용현황 비교

구 분	A은행	B증권	C카드
사용 방식	출금, 이체, 현금서비스 등	출금, 이체 등	물품 구입 등
사용 장소	사이버 거래	사이버 거래	가맹점/ 사이버 거래
SMS 대상	신청시 일정금액 이상	1천만 원 초과 거래 등	거래시마다
이용료	월 900원/계좌	무료	월 300원

주) 조사대상은 은행, 증권, 카드회사별 1개사를 선정하여 해당 금융회사 인터넷홈 페이지에서 조사함.

이와 같이 전자금융거래에서 발생할 수 있는 무권한 금융거래 등 금융사고를 예방 또는 축소하기 위하여 현재 금융소비자가 SMS 활용을 신청할 경우에만 이용할 수 있는 Opt-in 방식을 금융거래가 발생할 때마다 지속적으로 정보를 제공하는 Opt-out 방식으로 전환하여 전자금융거래의 투명성을 확보함으로써 위험 금융거래로 인한 금융사고를 예방할 수 있는 기회를 제공하는 것이 타당

하다 하겠다.

악의의 제 3자에 의한 불법적인 전자상거래 행위로 인한 금융소비자의 금융자산 인출시 전자상거래 업체를 상대로 거래 정보를 추적하여 통제하는 것은 현실적으로 어려움이 있으므로 전자상거래 및 금융거래 발생시 SMS 정보를 통보하도록 의무화하는 방법이 합리적인 것으로 판단된다.

이러한 적극적인 SMS 알림 서비스는 금융소비자에게 알권리 충족으로 금융사고의 사전 예방 및 금융자산의 안전성 확보뿐만 아니라, 금융회사는 해킹 또는 도덕적 해이 등 금융사고시 불법행위에 대한 고객의 인지 여부를 확인할 수 있으므로 금융사고 또는 민원과 소송 등 분쟁 발생시 금융회사의 무과실책임으로부터 구제할 수 있는 증빙자료로 활용될 수 있을 것이다.

5. 결 론

본 논문에서는 최근 전자금융거래법의 시행에 따른 금융사고 발생시 금융회사의 무과실책임 부여와 금융회사의 대응환경 변화에 대한 문제점으로 금융회사의 입증책임 부담, 금융소비자의 도덕적 해이에 의한 금융사고 개연성, 전자금융거래 복잡성 증가로 사고 원인 파악의 어려움 등을 분석해 보았다. 그리고 이러한 문제점에 대한 금융회사의 대응 현황과 금융소비자의 알권리 충족 및 금융사고 예방을 위한 금융거래정보의 활용 방안을 고찰하였다.

특히 본 연구에서 제안한 금융회사의 SMS 서비스의 Opt-out 방식으로의 전환을 통하여 금융소비자의 알권리 충족을 위한 금융자산 변경내역 정보를 제공함으로써 금융사고를 예방하거나 계속적인 사고를 차단할 수 있으며, 전자금융거래의 중요정보인 이용자 IP 정보를 활용함으로써 금융거래 발생장소 등을 이용한 위험거래인지 시스템의 운영은 금융회사뿐만 아니라 금융소비자 보호를 위한 사전적인 대응 방안이 될 수 있다고 판단된다. 또한, 금융거래 발생장소 정보는 금융소비자의 도덕적 해이에 의한 불법적인 금융사고가 발생하였을 경우 금융회사의 무과실 책임을 면할 수 있는 사고원인을 판단하는데 중요한 증빙자료로 활용될 수 있을 것이다.

개인정보 보호를 위하여 중요정보는 오남용과 유출사고에 대비하여 철저한 보안 관리를 하여야 하겠지만 전자금융 거래시 금융거래정보와 관련된 일부 개인정보를 제한적으로 활용함으로써 금융소비자와 금융회사 뿐만 아니라 사회 전반적으로 그 효익이 클 수 있다면 일부 완화할 필요성이 있다고 생각되며, 아울러 금융거래의 신뢰성, 안정성 및 투명성을 확보함으로써 금융소비자 보호 및 건전한 전자금융거래 활성화에 기여할 수 있을 것이다.

참 고 문 헌

[1] 한국인터넷진흥원, “2007년도 하반기 정보화 실태조사 결과자료”, 2008년 2월.

[2] 김인석, “전자금융사고 유형분석을 통한 정보보호정책에 관한 연구”, 고려대학교 정보경영 전문대학원 박사학위논문, 2008년 2월.

[3] 한미정, “전자금융사고의 책임원칙에 대한 연구”, 법제연구, 제32호, 2007년 6월.

[4] 정창모, ‘금융사고 : 사례와 대책’, 매일경제신문사, 2006.

[5] 금융감독원, “전자금융거래 안전성 강화 종합대책”, 2005.

[6] 금융감독원, “전자금융업자의 정보기술부문 등에 대한 안전성 확보방안”, 리스크 리뷰, 2006년 가을호.

[7] 금융감독원, “전자금융감독규정 해설”, 2007.

[8] 장병환, “전자금융거래에서 발생하는 소비자 보호 문제의 유형과 특징”, 금융결제원, 2007년 4월.

[9] 재정경제부, “전자금융거래법 설명 자료”, 2003년 8월.
[10] 국회 재정경제위원회, “전자금융거래법안에 관한 공청회 자료”, 2005년 6월
[11] 김자봉, “최근 전자금융의 발전과 주요 이슈”, 한국금융연구원, 2006년 6월.
[12] 정경영, “전자금융거래와 법”, 박영사, 2007.

조 성 인

1990년 충북대학교 전산통계학과
2007년 고려대학교 정보경영공학전문대학원 석사과정
현재 금융감독원 수석검사역

박 태 형

2004년 고려대학교 일반대학원 행정학과(석사)
2008년 고려대학교 정보경영공학전문대학원 박사과정 수료

임 종 인

1980년 고려대학교 수학과
1982년 고려대학교 수학과 (석사)
1986년 고려대학교 수학과 (박사)
2000년 고려대학교 자연과학대학 정교수
현재 고려대학교 정보경영공학전문대학원 원장, 고려대학교 정보보호기술 연구센터 센터장