전자금융거래법상 '이용자의 중과실'의 판단기준

- 대법원 2014.1.29. 선고 2013다86489 판결의 비판적 고찰 -

서 희 석*

≪目 次≫

〈국문요약〉

본 판결은 보이스피싱 등 전자금융사기로 인한 전자금융거래 이용자의 손해에 대한 금융기관의 법적 책임이 문제된 최초의 대법원 판결이라는 점에서 중요한 의의를 갖는다. 본 판결에서 대법원은 전자금융거래법상 금융기관의 면책요건으로 규정된 "이용자의 고의 또는 중과실"이 있는지 여부는 "접근매체의 위조 등 금융사고가 일어난 구체적인 경위, 그 위조 등 수법의 내용 및 그 수법에 대한 일반인의 인식 정도, 금융거래 이용자의 직업 및 금융거래 이용경력 기타 제반 사정을 고려하여 판단"하여야 한다는 판단기준을 제시하고, 이 기준에 따라 본 사안에서 이용자에게는 중과실이 있고 따라서 금융기관은 면책된다고 판단하였다. 그러나 본 판결에 대하여는, 금융거래정보 노출을 접근매체의 노출과 동일시하고 있으나 이것은 전자금융거래법의 문리적 해석범위를 넘는 것이라는 점, 제3자의 사기행위에 대한 평가가 거의 이루어지지 않았고 더욱이 금융기관의 보안수준은 아예 고려하지도 않았다는 점에서 찬성하기 힘

* 부산대학교 법학전문대학원 부교수.

들다. 향후에 대법원이 제시한 이용자의 중과실 판단기준에는 "금융기관의 전반적인 정보보안의 수준"이 추가되는 것이 타당하다고 생각한다. 이 기준이 추가된다면 금융기관의 정보보안이 취약할 경우에는 이용자의 중과실도 보다 신중하게 판단하도록 제어하는 역할을 하게 될 것이기 때문이다.

Ⅰ. 사안의 개요

1. 사실관계

(1) 원고는 '피고은행'(농협은행 및 서창농협)에 예금계좌(이하 위 농협은행 계좌를 '이 사건 제1예금계좌', 위 서창농협 계좌를 '이 사건 제2예금계좌'라 한다)를 개설하고 금융거래를 하면서 인터넷뱅킹 서비스를 이용해 왔다.

(2) 성명불상자는 2012. 3. 30. 원고에게 전화를 걸어 자신을 서울지방검찰청 검사라고 속이고 금융사기 범죄자를 검거하였는데 원고가 공범인지 확인이 필요하다면서 원고로 하여금 허위 대검찰청 인터넷 사이트에 접속하게 한 후 원고의 주민등록번호, 휴대전화번호, 신용카드번호(현대카드 및 신한카드), 예금계좌번호, 각 비밀번호, 보안카드번호, 보안카드 비밀번호를 각 입력하게 하였다.

(3) 위 성명불상자는 2012. 3. 30. 원고가 입력한 금융거래정보를 이용하여 원고 명의의 공인인증서를 재발급 받았고, 재발급 받은 공인인증서와 원고의 금융거래정보를 이용하여, 현대카드 주식회사로부터 현금서비스 1,800,000원, 카드대출 10,000,000원을 받고 이를 이 사건 제1예금계좌로 송금받아 위 돈과 이 사건 제1예금계좌의 예금액 합계 12,600,000원을 제3자 명의의 예금계좌로 송금하였고, 주식회

사 현대스위스2저축은행으로부터 10,000,000원, 주식회사 바로크레디트대부로부터 500,000원을 각 대출받고 이를 이 사건 제2예금계좌로 송금받아 위 돈과 이 사건 제2예금계좌의 예금액 합계 13,380,000원을 제3자 명의의 예금계좌로 송금하였다(이하 '이 사건 금융사고'라 한다).

2. 소송의 경과

(1) 원고의 청구취지 및 청구원인

원고는 이 사건 금융사고에 의해 자신의 예금계좌에서 인출된 손해배상금 합계 약 2600만원 및 이에 대한 소장부본 송달 다음날부터 갚는 날까지 연 20%의 비율로 이자를 지급하라는 소송을 제기하였는바, 아래와 같이 주위적으로는 전자금융거래법(2013.5.22. 법률 제11814호로 개정되기 전의 것. 이하 특별한 한정이 없는 한 이와 같다) 제9조 제1항[1]에서 정하는 금융기관의 책임을, 예비적으로는 민법 제760조 제3항이 규정한 과실에 의한 불법행위방조책임이 성립함을 주장하였다.

1) 전자금융거래법상 금융기관의 책임

공인인증서는 전자금융거래법 제9조 제1항에 규정된 '접근매체'에 해당한다고 할 것이고, 성명불상자가 원고의 정보를 부정하게 이용하여 공인인증서를 재발급 받는 행위도 전자금융거래법 제9조 제1항에서 말하는 '접근매체의 위조'에 포함된다고 할 것이므로, 이 사건 금융사고는 전자금융거래법 제9조 제1항에서 규정한 '접근매체의 위조로 발생한 사고'에 해당하므로, 금융기관인 피고은행은 특별한 사정이 없다면,

---

1) **전자금융거래법 제9조(금융기관 또는 전자금융업자의 책임)** ① 금융기관 또는 전자금융업자는 접근매체의 위조나 변조로 발생한 사고, 계약체결 또는 거래지시의 전자적 전송이나 처리과정에서 발생한 사고로 인하여 이용자에게 손해가 발생한 경우에는 그 손해를 배상할 책임을 진다.

전자금융거래법 제9조 제1항에 따라 원고에게 이 사건 금융사고로 발생한 손해를 배상할 책임이 있다.

2) 민법상 과실에 의한 불법행위방조책임

설사 전자금융거래법 제9조 제1항의 책임이 인정되지 않는다 하더라도 성명불상자가 원고 명의의 공인인증서를 재발급 받아 이 사건 금융사고를 저지를 때 피고은행이 원고에게 공인인증서 재발급 사실을 통지하여야 할 주의의무가 있으나 이를 게을리하여 결국 이 사건 금융사고를 방지하지 못하고 원고에게 손해를 입혔으므로 민법 제760조 제3항이 규정한 과실에 의한 불법행위방조책임에 따라 원고가 입은 손해를 배상할 책임이 있다.

(2) 피고은행의 항변

피고은행은 위와 같은 원고의 주장에 대해 다음과 같이 항변하였다.

1) 전자금융거래법상 금융기관의 책임에 대하여

이 사건 금융사고가 원고의 중대한 과실 때문에 발생한 것으로 전자금융거래법 제9조 제2항 제1호[2]와 동 제3항에 따른 시행령(2013.11.22. 대통령령 제24880호로 개

2) **전자금융거래법 제9조(금융기관 또는 전자금융업자의 책임)** ② 제1항의 규정에 불구하고 금융기관 또는 전자금융업자는 다음 각 호의 어느 하나에 해당하는 경우에는 그 책임의 전부 또는 일부를 이용자가 부담하게 할 수 있다.
1. 사고 발생에 있어서 이용자의 고의나 중대한 과실이 있는 경우로서 그 책임의 전부 또는 일부를 이용자의 부담으로 할 수 있다는 취지의 약정을 미리 이용자와 체결한 경우
2. 법인(「중소기업기본법」 제2조 제2항에 의한 소기업을 제외한다)인 이용자에게 손해가 발생한 경우로 금융기관 또는 전자금융업자가 사고를 방지하기 위하여 보안절차를 수립하고 이를 철저히 준수하는 등 합리적으로 요구되는 충분한 주의의무를 다한 경우
③ 제2항 제1호의 규정에 따른 이용자의 고의나 중대한 과실은 대통령령이 정하는 범위 안에서 전자금융거래에 관한 약관(이하 "약관"이라 한다)에 기재된 것에 한한다.

정되기 전의 것. 이하 다른 한정이 없는 한 이와 같다)[3] 및 관련 약관(전자금융거래 기본약관)[4]에 의거하여 피고은행의 책임이 전부 면제된다.

2) 민법상 불법행위방조책임에 대하여

공인인증서 발급시 피고은행이 원고에게 이를 휴대전화 문자메시지 등을 이용하여 통지할 주의의무가 존재한다고 보기 어렵고, 오히려 문자메시지 등을 이용한 통지는 피고은행이 이용자의 요청에 따라 제공하는 서비스로 보이는데 원고는 인터넷뱅킹 신청 당시 보안SMS 신청을 하지 않은 사실이 인정되며, 설령 피고들에게 그러한 주의의무가 있다고 하더라도 이를 이행하지 않음으로써 이 사건 금융사고가 발생하였다고 단정하기도 어렵다.

(3) 제1심의 판단

제1심은 위 피고은행의 항변을 모두 받아들여 원고의 청구를 기각하였다. 구체적 판시내용은 다음과 같다.

---

3) **전자금융거래법 시행령 제8조(고의나 중대한 과실의 범위)** 법 제9조 제3항에 따른 **고의나 중대한 과실의 범위**는 다음 각 호와 같다.

1. 이용자가 접근매체를 제3자에게 대여하거나 그 사용을 위임한 경우 또는 양도나 담보의 목적으로 제공한 경우(법 제18조에 따라 선불전자지급수단이나 전자화폐를 양도하거나 담보로 제공한 경우를 제외한다)
2. 제3자가 권한 없이 이용자의 접근매체를 이용하여 전자금융거래를 할 수 있음을 알았거나 쉽게 알 수 있었음에도 불구하고 접근매체를 누설하거나 노출 또는 방치한 경우

4) **전자금융거래 기본약관 제20조(손실부담 및 면책)** ① 농협은 접근매체의 위조나 변조로 발생한 사고, 계약체결 또는 거래지시의 전자적 전송이나 처리과정에서 발생한 사고로 인하여 이용자에게 손해가 발생한 경우에는 그 금액과 1년 만기 정기예금 이율로 계산한 경과이자를 보상한다.

② 제1항의 규정에도 불구하고 농협은 다음 각 호에 해당하는 경우에는 이용자에게 손해가 생기더라도 책임의 전부 또는 일부를 지지 아니한다.

3. 제3자가 권한 없이 이용자의 접근매체를 이용하여 전자금융거래를 할 수 있음을 알았거나 쉽게 알 수 있었음에도 불구하고 이용자가 자신의 접근매체를 누설 또는 노출하거나 방치한 경우

1) 전자금융거래법에 따른 금융기관의 손해배상책임 여부

"이 사건 금융사고 발생에 전자금융거래법 제9조 제2항 제1호가 규정한 이용자의 중대한 과실이 있는지 보건대, 앞서 인정한 사실에 의하면, 원고가 자신의 금융거래정보를 허위의 대검찰청 사이트에 입력함으로써 이를 성명불상자에게 노출하였고 성명불상자가 원고가 제공한 금융거래정보를 이용하여 원고의 공인인증서를 재발급받은 후에 이 사건 금융사고를 저지른 것이고, 또한 이른바 전화금융사기가 빈발함에 따라 이에 대한 사회적인 경각심이 높아진 상황을 고려할 때, 위와 같이 금융거래정보를 제3자에게 노출하면 제3자가 이를 가지고 권한 없이 이용자의 접근매체를 이용한 전자금융거래를 할 수 있다는 점을 일반인이라면 누구나 쉽게 예상할 수 있다고 할 것이므로, 결국 원고의 위와 같은 금융거래정보 노출행위는 전자금융거래법 제9조 제2항 제1호, 제3항, 같은 법 시행령 제8조 제2호, 피고들의 전자금융거래 기본약관 제20조 제2항 제3호가 규정한 금융사고 발생에 이용자의 "중대한 과실"이 있는 경우에 해당한다고 할 것이다. 따라서 피고은행은 이 사건 금융사고 때문에 발생한 손해에 대하여 그 책임을 부담하지 않는다고 할 것이므로, 피고은행의 위 항변은 이유 있다." (하선은 필자)

2) 과실에 의한 불법행위방조책임의 성립 여부

"성명불상자가 코스콤[공인인증기관]으로부터 원고 명의로 공인인증서를 재발급받은 사실은 당사자 사이에 다툼이 없는바, 이러한 사실에 비추어 볼 때, 제시된 증거의 각 기재만으로 공인인증서 발급시 피고은행이 원고에게 이를 휴대전화 문자메시지 등을 이용하여 통지할 주의의무가 존재한다고 보기 어렵고, 설령 피고은행에게 그러한 주의의무가 있다고 하더라도 이를 이행하지 않음으로써 이 사건 금융사고가 발생하였다고 단정하기도 어려우며, 달리 이 사건 금융사고와 관련하여 피고은행의 배상책임을 인정할 증거나 사정이 보이지 않는다(아울러 피고은행에게 이 사건 금융사고와 관련하여 전자금융거래법이 규정한 선관주의의무를 위반하였다고 보기도 어렵다). 따라서 원고의 위 주장은 이유 없다."

(4) 원심의 판단

원고가 항소하였으나, 원심도 제1심과 거의 같은 이유로 항소를 기각하였다. 다만 그 판단근거는 제1심에 비하여 다소 구체화되었다. 원심의 판시내용은 다음과 같다.

1) 전자금융거래법에 따른 손해배상책임의 인정 여부

"이 사건 금융사고 발생에 전자금융거래법 제9조 제2항 제1호가 규정한 이용자의 중대한 과실이 있는지 살피건대, 제시된 증거의 각 기재에 변론 전체의 취지를 종합하여 인정되는 다음과 같은 사정들 즉, ① 이 사건 금융사고 당시에는 이른바 전화금융사기가 빈발하여 이에 대한 사회적인 경각심이 높아진 상태였던 점, ② 원고는 이 사건 금융사고 당시 만 33세로서 공부방을 운영하는 등 사회경험이 있었고 1년 이상 인터넷뱅킹을 사용해왔던 점, ③ 원고는 관련 형사 사건의 조사과정에서 성명불상자로부터 '001'로 시작되는 국제전화를 받아 순간 이상하다는 생각을 하였다고 진술하고 있는 점, ④ 그럼에도 원고는 제3자에게 접근매체인 공인인증서를 발급[하는 데]에 필수적인 계좌번호, 계좌비밀번호, 주민등록번호, 보안카드번호, 보안카드비밀번호를 모두 알려준 점 등에 비추어 보면, 원고는 제3자가 권한 없이 접근매체를 이용하여 전자금융거래를 할 수 있음을 알았거나 쉽게 알 수 있었음에도 이를 노출하였다고 볼 것이므로, 결국 원고의 위와 같은 금융거래정보 노출행위는 전자금융거래법 제9조 제2항, 제3항, 같은 법 시행령 제8조 제2호, 피고들의 전자금융거래 기본약관 제20조 제2항 제3호가 규정한 금융사고 발생에 이용자의 '중대한 과실'이 있는 경우에 해당한다 할 것이므로, 피고은행의 위 항변은 이유 있다."(하선은 필자)

2) 과실에 의한 불법행위방조책임 성립 여부

"갑 제6, 7, 8호증(가지번호 포함)의 각 기재만으로는 피고은행에게 공인인증서 재발급시 원고에게 이를 문자메시지 등을 이용하여 통지할 주의의무가 존재한다고 보기 어렵고, 오히려 을 제7호증의 기재에 변론 전체의 취지를 종합하면, 문자메시지

등을 이용한 통지는 피고들이 이용자의 요청에 따라 제공하는 서비스로 보이는데 원고는 인터넷뱅킹 신청 당시 보안SMS 신청을 하지 않은 사실이 인정되며, 설령 피고 은행에게 그러한 주의의무가 있다고 하더라도 이를 이행하지 않음으로써 이 사건 금융사고가 발생하였다고 단정하기도 어려우므로, 원고의 위 주장은 이유 없다."

3. 대법원의 판단

원고의 상고에 대하여 대법원은 원심의 판단에 법리오해의 위법이 없다는 점을 들어 상고를 기각하였다. 대법원의 구체적 판시내용은 다음과 같다.

(1) 전자금융거래법에 따른 손해배상책임의 인정 여부

"전자금융거래법 및 동 시행령이나 전자금융거래 기본약관의 각 조항에서 정하는 '고의 또는 중대한 과실'이 있는지 여부는 접근매체의 위조 등 금융사고가 일어난 구체적인 경위, 그 위조 등 수법의 내용 및 그 수법에 대한 일반인의 인식 정도, 금융거래 이용자의 직업 및 금융거래 이용경력 기타 제반 사정을 고려하여 판단할 것이다. (중략) 앞서 본 법리에 비추어 살펴보면, [피고들의 전부 면책 주장을 받아들인] 원심의 위와 같은 판단은 정당한 것으로 수긍할 수 있고, 거기에 상고이유의 주장과 같이 위 법규정 등에서의 '중대한 과실' 또는 면책의 범위에 관한 법리를 오해하는 등으로 판결에 영향을 미친 위법이 있다고 할 수 없다."

(2) 과실에 의한 불법행위방조책임 성립 여부

"관련 법리에 비추어 기록을 살펴보면, 원심의 판단은 정당하고, 거기에 상고이유의 주장과 같이 불법행위의 방조에 관한 법리를 오해한 위법이 있다고 할 수 없다."

II. 문제제기

1. 본 사안의 쟁점 및 대법원의 결론

본 사안의 쟁점은 이른바 보이스피싱(voice phishing)으로 대표되는 전자금융사기에서 전자금융거래법상 금융기관의 면책요건으로 규정된 '이용자의 중과실'을 인정할 수 있는지 여부와, 공인인증서 재발급과 관련하여 금융기관에게 공동불법행위의 방조책임을 인정하기 위한 주의의무 위반이 인정되는지 여부의 두 가지로 요약된다. 이에 대한 대법원의 판단은 요컨대 이용자에게는 전자금융거래법상 중과실이 인정되고, 금융기관에게는 주의의무 위반(과실)이 인정되지 않는다는 것이다.

먼저 전자, 즉 본 사안에서 문제가 된 전자금융거래법상 이용자의 중과실의 판단기준에 관하여 대법원은, "전자금융거래법 및 동 시행령이나 전자금융거래 기본약관의 각 조항에서 정하는 '고의 또는 중대한 과실'이 있는지 여부는 접근매체의 위조 등 금융사고가 일어난 구체적인 경위, 그 위조 등 수법의 내용 및 그 수법에 대한 일반인의 인식 정도, 금융거래 이용자의 직업 및 금융거래 이용경력 기타 제반 사정을 고려하여 판단할 것이다."라는 일반론을 전개한 후 이와 같은 판단기준에 입각하여 판단할 때 본 사안에서 원고에게 중대한 과실을 인정할 수 있다는 원심의 판단은 정당하다고 판시하였다. 이에 따라 피고은행은 전자금융거래법 및 관련 약관에 따라 전부면책된다는 원심판단이 확정되었다. 이어서 후자, 즉 금융기관의 주의의무 위반과 관련하여서는 제출된 증거로부터 판단할 때 피고은행에게 공인인증서 재발급시 원고에게 이를 문자메시지 등을 이용하여 통지할 주의의무가 존재한다고 보기 어렵고, 원고는 인터넷뱅킹 신청 당시 보안SMS 신청을 하지 않았고, 설사 피고은행에 그러한 주의의무가 있다고 하더라도 피고은행이 위 주의의무를 이행하지 않음으로써 이 사건 금융사고가 발생하였다고 단정하기도 어려우므로, 원고의 위 주장은 이유 없다고 판시하였다. 이에 따라 피고은행에 불법행위의 방조책임이 인정될 수 없다는 원심판단이 확정되었다

2. 접근매체의 노출이 있었는가?

그러나 대법원의 이와 같은 판단에는 선뜻 납득하기 어려운 점들이 있다.

우선 이용자의 중과실 판단과 관련하여서는 대법원은 전자금융거래법에서 이용자의 중과실의 범위로 규정하는 이용자에 의한 "접근매체[5](특히 공인인증서)의 노출"(전자금융거래법[6] 시행령 제8조 제2호)이 있었다고 보아 이로부터 원고의 중과실을 인정하고 있는데 본 사안에서 원고는 공인인증서 자체는 노출하지 않고 있다는 점이다. 즉 원고가 노출한 것은 신용카드정보 및 그 비밀번호, 은행계좌번호 및 보안카드번호 등의 금융거래정보일 뿐 전자금융거래에서 필수적으로 요구되는 공인인증서(법 제2조 10호 나목) 및 그 비밀번호(동 마목)는 노출하지 않고 있는 것이다. 그런데 이 점에 관하여 제1심은 "금융거래정보를 제3자에게 노출하면 제3자가 이를 가지고 권한 없이 이용자의 접근매체를 이용한 전자금융거래를 할 수 있다"고 하여 금융거래정보와 접근매체의 관계에 관하여는 명시하지 않은 채 양자를 혼동하고 있는 듯한 판시를 하고 있고, 원심 및 대법원은 "제3자에게 접근매체인 공인인증서의 발급에 필수적인 계좌번호, 계좌비밀번호, 주민등록번호, 보안카드번호, 보안카드비밀번호를 모두 알려준 점 등에 비추어 보면, 원고가 제3자가 권한 없이 접근매체를 이용하여 전자금융거래를 할 수 있음을 알았거나 쉽게 알 수 있었음에도 이를 노출하였다고 볼 것"이라고 하여 금융거래정보의 노출을 접근매체의 노출과 동일시하고 이를 근거로 원고의 중과실을 이끌어내고 있다. 다시 말하면 원심 및 대법원은 금융거래정

---

5) 전자금융거래법 제2조 10. "접근매체"라 함은 전자금융거래에 있어서 거래지시를 하거나 이용자 및 거래내용의 진실성과 정확성을 확보하기 위하여 사용되는 다음 각 목의 어느 하나에 해당하는 수단 또는 정보를 말한다.
가. 전자식 카드 및 이에 준하는 전자적 정보
나. 「전자서명법」 제2조 제4호의 전자서명생성정보 및 같은 조 제7호의 인증서
다. 금융회사 또는 전자금융업자에 등록된 이용자번호
라. 이용자의 생체정보
마. 가목 또는 나목의 수단이나 정보를 사용하는데 필요한 비밀번호

6) 이하 「전자금융거래법」을 인용할 경우에는 "법"이라고만 한다.

보를 이용하여 공인인증서를 발급받고 이를 이용하여 (무권한의) 전자금융거래를 할 수 있음을 원고가 쉽게 알 수 있었음에도 금융거래정보를 노출하였다는 점으로부터 원고의 중과실을 이끌어내고 있는 것이다.

그러나 접근매체인 공인인증서 및 그 비밀번호의 노출이 없었음에도 불구하고 "공인인증서의 발급에 필수적"이라는 이유로 "금융거래정보의 노출이 곧 접근매체의 노출"이라는 해석이 가능한 것인지 의문이 없지 않다. 전자금융거래법은 이용자의 고의 또는 중과실의 범위로 "(제3자가 권한 없이 이용자의 접근매체를 이용하여 전자금융거래를 할 수 있음을 알았거나 쉽게 알 수 있었음에도 불구하고) 접근매체를 누설하거나 노출 또는 방치한 경우"로 명시하고 있기 때문에(시행령 제8조 제2호) 문리적으로 접근매체가 아닌 금융거래정보를 노출한 경우를 접근매체의 노출과 동일시할 수는 없기 때문이다. 그렇다면 본 사안에서는 접근매체가 노출된 것이 아니라 노출된 금융거래정보를 이용하여 '접근매체를 위조'(전자금융거래법 제9조 제1항 제1호)하거나 접근매체를 부정한 방법으로 재발급받은 것이 문제된 사안은 아닌지 검토해볼 여지가 있다고 할 것이다.

3. 성명불상자의 기망행위에 대한 평가

원심 및 대법원의 판결은 본 사안에서 성명불상자에 의한 전자금융사기 수법 내지 기망행위에 대한 법적 평가가 누락되어 있는 것은 아닌지 검토의 여지가 있다. 원고는 검사라고 사칭하는 자로부터 기망을 받아 자신의 금융거래정보를 노출한 것이다. 일반인의 입장에서는 검사라 사칭하는 자로부터의 전화에는 당황하기 마련이다. 더욱이 (판결문에는 명시되어 있지 않으나 동종 유사사건으로부터 판단할 때) 검사사칭자는 먼저 자신이 ○○지검의 검사 아무개라는 점을 고지하고, 피해자에게 피해자의 계좌가 ○○ 은행에 있지 않느냐는 점의 확인을 요구한 후,[7] 이어서 그 계좌가

7) 보통 그 이전에 피해자의 개인정보 및 금융정보를 (부정한 수단으로) 확보하고 있을 개연성이 대단히 높다.

전자금융사기에 연루되어 있다거나 피해자가 전자금융사기 범죄의 공범은 아닌지 확인할 필요가 있다는 등의 허위의 사실을 고지한다. 이러한 상황에서라면 일반인의 입장에서라면 불안한 마음에 검사사칭자의 지시대로 움직일 수밖에 없는 측면이 있다. 그렇다면 자신의 금융거래정보를 검사사칭자의 지시대로 허위의 대검찰청 사이트에 입력하였다는 점에서 원고의 행위에 과실이 있다는 점은 인정할 수 있다 하더라도, 그것이 '중과실'로까지 평가될 수 있는지는 의문이 없지 않다.

이점에 관하여는 본 사안의 전자금융사기 수법이 원심 및 대법원이 설시하듯 전자금융사기에 대한 사회적 경각심이 높아진 상태였기 때문에 원고의 중과실을 인정할 정도로 쉽게 알 수 있는 정도의 것이었는지 전자금융사기 수법의 실태 내지 기망행위로서의 특징을 살펴볼 필요가 있다. 아울러 외국 법제에서 이용자의 중과실 판단은 어떻게 이루어지고 있는지 비교법적인 검토가 필요하다. 한편 기망행위가 개입된 경우의 피기망자의 중과실 판단에 관하여는 착오취소에서의 착오자의 중과실(민법 제109조 제1항 단서) 판단에 관한 대법원 판례의 태도가 참조될 수 있다고 생각한다.

4. 공인인증서의 발급절차상의 문제점

원심 및 대법원과 같이 "공인인증서의 발급에 필수적"이기 때문에 "금융거래정보의 노출이 곧 접근매체의 노출"이라는 해석이 성립하기 위해서는 실제적으로 원고가 노출한 금융거래정보를 이용하여 공인인증서가 발급될 수 있어야 할 터인데, 본 사안에서는 공인인증서가 어떻게 하여 '재발급'될 수 있었는지에 관하여는 아무런 설시가 없고, 다만 원심 및 대법원은 접근매체(공인인증서)의 재발급을 所與의 전제로 하고 있을 뿐이다. 이점에 관하여 공인인증서의 발급절차를 규정하는 전자서명법은 공인인증서의 발급시에 대면에 의한 신원(실명 및 본인)확인이 필요함을 명시하고 있고, 전자금융거래법도 접근매체의 발급 시에 본인확인을 요구하고 있는바(제6조 제2항),

이때의 본인확인도 법에서 명시하는 예외사유가 아닌 한[8] 주민등록증 등의 대면에 의하여야 하는 것으로 해석된다. 따라서 이와 같은 원칙에 따른다면 예금계좌번호 등의 금융거래정보가 노출되었다고 하더라도 대면에 의한 본인확인이 이루어지는 한에서는 (예컨대 주민등록증 등을 위조하지 않는 한) 접근매체의 발급은 사실상 불가능하다고 하여야 할 것이다.

문제는 2006년 6월 30일에 개정(동년 7월 1일 시행)된 「전자서명법 시행규칙」에서 전자금융거래의 경우에는 그 "편의성을 높이기 위하여"[9] 공인인증서 발급을 정보통신망을 통하여 할 수 있도록 하는 예외규정을 신설하였다는 점이다(제13조의2 제4항)(동 규정에 대한 상세한 설명은 후술하는 Ⅲ.2.(2)2)를 참조). 이 규정에 의하면 전자금융거래 가입자는 계좌번호와 비밀번호 및 주민등록번호 등의 몇 가지 정보만으로도 공인인증서를 발급받을 수 있게 된다. 원심과 대법원이 위와 같은 시행규칙상의 예외규정에 입각하여 원고가 노출한 금융거래정보가 "공인인증서의 발급에 필수적"이라고 판단하였는지는 알 수 없다. 그러나 이와 같은 명문 규정이 존재하므로 실무에서는 공인인증서가 몇몇 금융거래정보만으로 정보통신망을 통하여 발급되고 있고 본 사안에서도 그와 같은 방식으로 재발급되었다는 점을 추론해 볼 수는 있다. 그렇다면 전자금융거래의 '편의성'이라는 이유로 도입된 공인인증서 발급절차의 예외규정을 어떻게 평가할 것인가? 만일 원칙대로 공인인증서의 발급절차로서 대면에 의한 본인확인절차가 고수되었다면 본 사안과 같은 전자금융사기가 발생할 수 있었을까? 본 사안의 두 번째 쟁점과 관련한 원고의 주장, 즉 피고은행이 원고에게 공인인증서 재발급 사실을 통지하여야 할 주의의무가 있다는 주장은 이와 같은 점에서 쉽게 배척하기 어려운 설득력을 내포하고 있다고 생각한다. 공인인증서를 통한 전자금융거래라는 우리나라 특유의 법제도는 제도 시행 당시(2007년 1월 1일)부터 이미

8) 전자금융거래법 제6조 제2항 단서는 본인확인을 요하지 않는 예외사유로서, 1. 선불전자지급수단이나 전자화폐인 경우 및 2. 접근매체의 갱신 또는 대체발급 등을 위하여 이용자의 동의를 얻은 경우를 들고 있다.

9) 법제처 「전자서명법 시행규칙」 (2006.6.30. 개정) 개정이유 참조.

근본적인 보안의 문제(정확하게는 법제도상의 문제)를 안고 있었던 것이라고 평가할 수 있기 때문이다.

이하에서는 이러한 문제의식에 입각하여, 위에서 제기한 세 가지 문제를 검토하기로 한다(Ⅳ). 검토에 앞서 본 판결의 결론에 가장 커다란 영향을 미친 '접근매체'의 의의 및 법적 효력에 관하여 이론적으로 정리하는 작업을 선행한다(Ⅲ). 전자금융거래의 기술적 구조에 대한 이해가 관련된 법적 판단에 있어서도 필수적이라고 생각되기 때문이다.

Ⅲ. 접근매체의 의의 및 법적 효력

1. 전자금융거래에서 접근매체의 의의

(1) 전자금융거래의 구조-시스템거래[10)]

'전자금융거래'는 금융상품 및 서비스가 제공되는 전자적 장치를 통하여 비대면의 자동화된 방식에 의해 이루어지는 거래로 정의된다(법 제2조 제1호 참조). 여기서 금융상품 등이 제공되는 '전자적 장치'란 "전자금융거래정보를 전자적 방법으로 전송하거나 처리하는데 이용되는 장치"로서 현금자동지급기(CD), 자동입출금기(ATM), 지급용단말기, 컴퓨터, 전화기 등이 포함된다(법 제2조 제8호). 이 전자적 장치가 곧 '전자금융거래 시스템'이라 할 수 있다. 그런데 이와 같은 전자적 장치는 통신회선(망)에 의해 네트워크화될 때 비로소 전자금융거래정보의 전자적 전송이 가능해지고 격지자간의 전자금융거래가 성립한다. 따라서 전자금융거래 시스템이란 위와 같은 의미의 전자적 장치와 통신회선(망)을 포괄하며, 또한 이른바 하드웨어뿐만 아니라 정보처리 등을 가능하게 하는 소프트웨어를 아우르는 개념이다. 그렇다면 전자금융

10) 시스템거래 및 접근매체에 관한 기본적 생각은, 徐熙錫「電子金融取引の民事法理(3・完)-韓国電子金融取引法の考察-」一橋法学第6巻第3号(2007.11)196頁以下를 참조하였다.

거래는 이와 같은 의미의 '시스템'에 의한 거래라는 의미에서 '시스템거래'라 할 수 있다.

개별적인 전자금융거래는 전자금융거래를 위한 시스템(전자금융거래 시스템)에의 접근으로부터 시작된다. 전자금융거래의 발달단계에서 볼 때 그 초기에는 금융기관만이 시스템에 접근할 수 있었으나,[11] 기술의 발달로 이용자가 직접 시스템에 접근하여 전자금융거래를 할 수 있는 시대가 도래하였다(ATM, 인터넷뱅킹 등). 이용자가 시스템에의 접근을 위하여 필요한 것이 '접근매체'이다. 예를 들면, ATM에 의한 예금인출거래를 위해서는 현금카드와 비밀번호가 필요하며, 인터넷뱅킹에 의한 자금이체거래를 위해서는 이용자ID와 비밀번호 또는 공인인증서와 비밀번호가 필요하다. 여기서 현금카드, 비밀번호, 이용자ID, 공인인증서 등이 이른바 접근매체에 해당하는 것인데, 이들 접근매체에 의하여 이용자는 전자금융거래 시스템(이하 단순히 '시스템'이라고도 한다)에 접근하는 것이 허용되는 것이다. 접근매체의 삽입(카드나 USB 등)과 입력(정보) 등에 의해 시스템에의 접근이 허용된 이용자는 예금인출이나 자금이체를 위한 거래지시를 입력하고 이를 전송함으로써 거래가 완성된다.[12] 이상은 예금인출거래나 자금이체거래의 기술적 구조를 설명한 것이지만 다른 전자금융거래에서도 기본적인 기술적 구조는 마찬가지이다.

그렇다면 우리법상 접근매체는 어떻게 정의되고 그 종류에는 무엇이 있는가?

(2) 접근매체의 定義

전자금융거래법상 접근매체는 "전자금융거래에 있어서 거래지시를 하거나 이용자 및 거래내용의 진실성과 정확성을 확보하기 위하여 사용되는 수단 또는 정보"로 정의된다(법 제2조 제10호 참조).

---

11) 예컨대 은행 간의 자금이체거래에서 초기에는 은행 직원만이 시스템(은행간 자금이체시스템)에의 접근이 허용되었다.

12) 법적으로는 인터넷뱅킹에서의 거래지시(정보)의 도달(수취인 은행의 입금기록)이나 ATM에서의 수취인의 현금 수령 시점에 지급으로서의 효력이 발생한다(법 제13조).

전술한 바와 같이 접근매체는 문리적으로는 "(시스템에) 접근하기 위한 매체"를 의미한다. 시스템에 접근할 수 있다는 것은 시스템에 접근함으로써 거래지시를 할 수 있다는 의미이다. 따라서 접근매체는 전자금융거래법에서 최소한 "(시스템에 접근하여) 거래시시를 하기 위한 수단이나 정보"로 정의된다. 그런데 전자금융거래법은 여기서 더 나아가 "이용자 및 거래내용의 진실성과 정확성을 확보하기 위한 수단 또는 정보"로서도 접근매체를 정의한다. 따라서 전자금융거래법상의 접근매체는 ①시스템에 접근하여 거래지시를 하기 위한 수단 또는 정보(접근매체로서의 기능), ②이용자의 진실성과 정확성을 확보하기 위한 수단 또는 정보(본인확인 수단으로서의 기능) 및 ③거래내용의 진실성과 정확성을 확보하기 위한 수단 또는 정보(거래 무결성의 확인수단으로서의 기능)라는 세 가지 기능을 가질 수 있는 매체로 정의되고 있음을 알 수 있다.

(3) 접근매체의 종류

이와 같이 전자금융거래법은 접근매체에 세 가지 기능이 있을 수 있음을 전제로 이에 해당하는 매체를 다음의 다섯 가지로 한정열거하고 있다(법 제2조 10호 가~마). 먼저 ①전자식 카드 및 이에 준하는 전자적 정보이다. 예컨대 선불카드나 전자화폐카드, 현금카드, 신용카드 등의 전자식 카드가 이에 해당하는데 이들은 시스템에의 접근을 허용하여 거래지시를 할 수 있게 한다. 뿐만 아니라 이에 준하는, 즉 이와 같은 기능을 가진 '전자적 정보'로서, 예컨대 전자화폐카드나 신용카드 등에 수록된 전자적 정보가 카드 외의 다른 저장매체(스마트폰 등)에 저장된 경우가 이에 해당한다.[13]

다음으로 ②「전자서명법」 제2조 제4호의 전자서명생성정보 및 같은 조 제7호의

13) 문리적으로는 "전자식 카드에 준하는 전자적 정보"도 이에 포함되므로, 전자식 카드에 관한 정보(카드번호 등) 그 자체도 시스템에의 접근을 가능하게 한다면 ①에 포함된다고 해석될 여지가 있으나, 정보 그 자체가 아니라 '전자적 정보'로 한정하였다는 점에 주의할 필요가 있다. 따라서 카드번호 등의 거래정보는 여기서의 전자적 정보에는 포함되지 않는다고 해석할 것이다.

인증서이다. '전자서명생성정보'라 함은 전자서명을 생성하기 위하여 이용하는 전자적 정보를 말하며, '인증서'라 함은 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보를 말한다. 이것은 마치 인감과 인감증명서와 같은 역할을 전자적 환경에서 구현하는 것으로 양자는 모두 '전자적 정보'이기 때문에 실무에서는 전자서명생성정보가 인증서에 탑재(수록)되는 형태로 운영되고 이용자는 전자문서에 이 인증서를 첨부함으로써 '전자서명'을 한 것으로 인정받게 된다. 전자서명이라 함은 "서명자를 확인하고 서명자가 당해 전자문서에 서명을 하였음을 나타내는데 이용하기 위하여 당해 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보"로 정의되기 때문이다(동법 제2조 제2호). 이로써 전자문서에 대하여 종이문서에서의 서명 또는 기명날인과 같은 효력이 발생한다(동법 제3조 제3항). 이와 같은 인증서를 공인인증기관에서 발급한 것이 '공인인증서'이고(동법 제2조 제8호), 공인인증서에 기초한 전자서명이 '공인전자서명'이다(동법 제2조 제3호). 그런데 전자금융거래의 실무에서는 전자금융거래를 하기 위해서는 공인인증서가 필요하기 때문에(이것은 금융감독당국의 정책에 의한 것이다) 여기서 "전자서명생성정보 및 인증서"는 실질적으로는 **"공인인증서에 의한 공인전자서명"**을 의미하는 것으로 이해할 것이다. 공인인증서에 따라 전자금융거래가 이루어진 경우에는 "서명자의 동일성"과 전자거래에 사용된 "전자문서의 완전성 내지 무결성(integrity)"이 추정된다.[14] 한편 공인인증서는 전자서명법상 본인확인의 수단으로서도 활용된다(동법 제18조의2).

다음은 ③**금융기관 또는 전자금융업자에 등록된 이용자번호**이다. 이것은 예컨대 금융기관 또는 전자금융업자(이하 양자를 합쳐 단순히 '금융기관'이라 한다)의 시스템에 접근(접속)하기 위하여 금융기관이 이용자번호를 등록받는 경우에 그 번호가 접근매체가 된다는 것을 의미한다. 그러나 거래의 실무에서 이용자번호만으로 시스

14) **전자서명법 제3조(전자서명의 효력 등)** ②공인인증서에 따라 공인전자서명이 이루어진 경우에는 당해 전자서명이 서명자의 서명, 서명날인 또는 기명날인이고, 당해 전자문서가 전자서명된 후 그 내용이 변경되지 아니하였다고 추정된다.

템에의 접근이 허용되거나 본인확인이 이루어지는 경우는 최근에는 사실상 거의 없다고 보아야 할 것이다(비밀번호가 추가되어야 하거나 공인인증서에 의한 본인확인을 요구하는 경우가 많다). ④는 **이용자의 생체정보**이다. 이것은 이용자의 지문이나 홍채 등의 생체정보를 디지털화하여 이를 시스템에의 접근에 활용하는 것을 염두에 둔 접근매체이다. 그러나 최근의 실무에서는 다른 접근매체와 함께 보조적으로 지문정보 등이 활용되는 예는 있으나 생체정보 자체만으로 시스템에의 접근이나 본인확인을 완료하는 경우는 거의 없다.[15] ⑤는 **①과 ②의 수단이나 정보를 사용하는데 필요한 비밀번호**이다. 전자식 카드나 공인인증서의 경우 현행 실무상으로는 그 자체만으로 접근매체로 기능할 수는 없고 그와 함께 비밀번호가 일치하여야 본인확인이 이루어지고 시스템에 접근하여 거래지시를 할 수 있다. 따라서 ⑤는 그 자체만으로는 접근매체로서 의미가 없기 때문에 ①과 ②의 보조적 수단이라고 이해할 것이다.

이와 같이 전자금융거래법상 접근매체는 5가지로 한정열거되어 있으나 사실상은 4가지라고 볼 것이다(①⑤, ②⑤, ③, ④). 그런데 ③과 ④의 경우 접근매체로 정의되어 있으나 단독으로 시스템에의 접근이 허용되거나 본인확인이 완료되는 예는 현재의 실무상으로는 거의 없고 다른 접근매체와 함께 또는 보조적 수단으로 활용되고 있을 뿐이다. 그렇다면 현행 실무에서 접근매체로 사실상 중요한 의미를 갖는 것은 ①과 ② 및 각각의 경우의 비밀번호(⑤)라고 할 것이다.[16]

---

15) 생체정보만으로 시스템에의 접근을 허용하는 최근의 예로서, (전자금융거래에서의 사안은 아니지만) 무인 물품보관장치를 생각할 수 있다. 철도역 등에 설치된 일부 무인 물품보관장치에서는 이용자의 지문정보 만으로 물품보관 시스템에의 접근을 허용하고 있다.

16) 현행 실무에서 접근매체로서 ①전자식 카드와 ⑤비밀번호가 사용되는 경우로서 예컨대 현금카드와 비밀번호를 통한 ATM에서의 예금인출거래를 생각할 수 있다. 이 경우 이용자는 현금카드와 비밀번호만 있으면 ATM에서 예금을 인출할 수 있고, 현금을 수령하는 순간에 지급의 효력이 발생한다(전자금융거래법 제13조 제2호). 한편 ②와 ⑤는 이른바 인터넷뱅킹으로 대표되는 전자지급거래나 비대면 대출거래 등을 위하여 실무상 필수적으로 요구되는 접근매체로서 이것이 없으면 시스템에의 접근자체가 허용되지 않는다는 점에서 대단히 중요한 접근매체이다. 본 사안에서 성명불상자가 신용카드회사로부터 비대면 대출거래를 통하여 거액의 금액을 원고의 예금계좌

(4) 접근매체의 실무상 의의

전술한 바와 같이 접근매체는 전자금융거래를 위한 시스템에의 접근을 위한 수단이나 정보라는 점에 그 실무상 의의가 있으나, 더욱 중요한 것은 전자금융거래에서는 접근매체를 통한 거래지시(의사표시의 일종이다)의 법적 효과가 그 접근매체상의 본인에게 직접 미친다는 점이다(본인효과귀속성). 이것은 네트워크를 통하여 전송된 '전자문서'(정보처리시스템에 의하여 전자적 형태로 작성, 송신·수신 또는 저장된 정보)에 포함된 의사표시의 법적 효과에 관하여 규율하는 「전자문서 및 전자거래기본법」 제7조 제2항에 따른 결과이고, 이 규정은 전자금융거래를 위하여 사용되는 전자문서에 대하여도 그대로 적용되기 때문이다(법 제5조 제1항). 즉, "전자문서의 수신자는 전자문서가 작성자의 것이었는지를 확인하기 위하여 수신자가 미리 작성자와 합의한 절차를 따른 경우 전자문서에 포함된 의사표시를 작성자의 것으로 보아 행위할 수 있다"(전자문서 및 전자거래기본법 제7조 제2항). "접근매체의 이용"은 "(본인확인 등을 위하여) 수신자가 미리 작성자와 합의한 절차"에 해당하므로 접근매체에 의해 시스템에 접근한 후 거래지시로서 전자문서가 송신·수신된 경우 수신자(금융기관)는 당해 의사표시를 접근매체상의 본인(이용자)의 것으로 보고 행위하는 것이 가능하게 된다. 이것은 당해 의사표시의 법적 효과가 접근매체상의 본인(이용자)에게 미치는(또는 효력부정을 방지하는) 근거규정이 된다. 따라서 어느 이용자가 자신의 접근매체를 타인에게 사용하게 한 경우 그 접근매체에 의해 이루어진 전자금융거래는 기본적으로 이용자(접근매체상의 본인)에게 그 효과가 귀속된다는 점에 주의할 필요가 있다(본인효과귀속성).

요컨대 접근매체는 비대면거래로서의 전자금융거래를 위해서는 없어서는 안 되는 관문과 같은 존재이나, 그 관리가 잘못될 경우에는 그 효과가 본인에게 귀속될 위험성이 존재한다. 따라서 접근매체의 이상과 같은 특성(본인효과귀속성)으로부터 접근

로 이체받고, 이를 다른 예금계좌로 이체함으로써 편취할 수 있었던 것은 공인인증서를 '재발급'받을 수 있었기 때문에 가능한 것이었다.

매체의 발급자는 그 발급시에 본인확인을 철저히 하여야 하며, 접근매체를 발급받은 이용자는 접근매체에 대하여 관리상의 주의를 다하여야 한다. 전자금융거래법이 다음 항에서 보는 바와 같이 접근매체에 대하여 발급 및 관리상의 주의의무에 관한 규정을 두고 있는 것은 이와 같은 이유 때문이다.

2. 접근매체의 발급 및 관리상의 주의의무

(1) 서설

전자금융거래에서 접근매체의 실무상 의의를 위와 같이 이해하는 한 접근매체는 대면에 의한 본인확인절차를 철저히 거친 후에 발급되어야 하며, 한번 발급된 접근매체는 타인에 의해 사용되지 않도록 그 관리에 주의를 다하여야 한다는 것은 자명한 귀결이다. 전자금융거래법은 이점에 관하여 금융기관에 대하여는 접근매체의 발급에 관한 주의의무를, 이용자에 대하여는 접근매체의 사용 및 관리에 관한 주의의무를 각각 규정한다. 이하 분설한다.

(2) 접근매체의 발급상의 주의의무

1) 전자금융거래법—금융기관

금융기관이 접근매체를 발급할 때에는 "이용자의 신청이 있는 경우에 한하여 본인임을 확인한 후에" 발급하여야 한다"(법 제6조 제2항). 여기서 본인임을 확인하는 방법 및 절차가 문제되는데, 전자금융거래법에는 이에 관한 명문의 규정이 없다. 생각건대 전자금융거래에서 접근매체 발급의 중요성으로부터 여기서의 본인확인은 "대면에 의한 확인"을 의미하는 것으로 해석할 것이다. 이때 보통은 주민등록증 등 신분확인이 가능한 증표에 의하여 실명 및 본인임을 확인하여야 할 것인데,[17] 이때 금융

17) 참고적으로 「금융실명거래 및 비밀보장에 관한 법률」에서는 금융거래의 실명확인은 기본적으로 주민등록증에 의하여 이루어져야 함을 명시하고 있고(제3조 제1항, 시행

기관에 요구되는 주의의무의 정도는 주민등록증의 진정 여부를 확인함과 동시에 그 사진과 실물을 대조하는 등 그 직무수행상 요구되는 충분한 주의의무라고 할 것이다(판례).[18] 이와 같이 접근매체는 이용자의 신청이 있는 경우에 한하여 대면에 의한 본인확인을 철저히 한 후에 발급하는 것이 원칙이나, ①선불전자지급수단이나 5만원 이하의 전자화폐의 경우나 ②접근매체의 갱신이나 대체발급 등을 위하여 대통령령이 정하는 바에 따라 이용자의 동의를 얻은 경우[19]에는 이용자의 신청이나 본인의 확인

규칙 제3조 참조), 「전자서명법」에서는 공인인증서 발급시의 신원확인 절차로서 직접 대면하여 기본적으로 주민등록증에 의하여 실명 및 본인임을 확인하여야 한다는 점을 명시하고 있다(제15조, 시행규칙 제13조의2 제2항).

18) 폰뱅킹(phone-banking; telebanking)에 의한 자금이체 사기사건에서 〈대법원 1998.11.10. 선고 98다20059 판결〉은 "자금이체신청의 경우에는 은행의 창구직원이 직접 손으로 처리하는 경우와는 달리 그에 따른 자금이체가 기계에 의하여 순간적으로 이루어지지만, 그것이 채권의 준점유자에 대한 변제로서 은행에 대하여 요구되는 주의의무를 다하였는지 여부를 판단함에 있어서는, 자금이체시의 사정만을 고려할 것이 아니라 그 이전에 행하여진 폰뱅킹의 등록을 비롯한 제반 사정을 총체적으로 고려하여야 하며, 은행이 거래상대방의 본인 여부를 확인할 필요가 있는 경우에 담당직원으로 하여금 그 상대방이 거래명의인의 주민등록증을 소지하고 있는지 여부를 확인하는 것만으로는 부족하고 그 직무수행상 필요로 하는 충분한 주의를 다하여 주민등록증의 진정 여부 등을 확인함과 아울러 그에 부착된 사진과 실물을 대조하여야 할 것인바, 만일 실제로 거래행위를 한 상대방이 주민등록상의 본인과 다른 사람이었음이 사후에 밝혀졌다고 한다면, 특별한 사정이 없는 한, 은행으로서는 위와 같은 본인확인의무를 다하지 못한 과실이 있는 것으로 사실상 추정된다."고 하였다. 이 판시는 전자금융거래 전체에 그대로 타당하다고 생각한다.

다만 〈대법원 2006.12.21. 선고 2004다41194 판결〉에서는 PC뱅킹의 등록에 요구되는 은행의 주의의무에 대하여 "거래처가 통장으로 예금을 찾을 때 예금지급을 위하여 요구되는 주의의무(예금거래기본약관에 의하면, 은행은 예금지급청구서 등에 찍힌 인영(또는 서명)을 신고한 인감(또는 서명감)과 주의 깊게 비교·대조하여 틀림없는지와 예금지급청구서 등에 적힌 비밀번호가 신고한 것과 동일한지를 확인하여야 한다)와 동일한 정도로 주의"가 필요하고 "등록 이후에도 비밀번호 등이 누설되어 예금의 인출이 되지 않도록 주의하여야 할 의무가 있다."고 판시하여 등록 시 요구되는 주의의무의 정도를 다소 완화한 듯한 판시를 하고 있다.

19) 시행령 제6조(접근매체의 갱신 또는 대체발급) 1. 갱신 또는 대체발급 예정일 전 6월 이내에 사용된 적이 없는 접근매체는 이용자로부터 갱신 또는 대체발급에 대하여

이 없는 때에도 접근매체를 발급할 수 있다(법 제6조 제2항 단서). 이와 같은 예외를 둔 이유는, ①은 선불식 교통카드 등 소액결제에 주로 사용되는 선불식 전자지급수단으로서 이 경우에는 특히 본인확인이 필요없다고 판단했기 때문이고, ②는 접근매체의 갱신 등에서 미리 이용자의 동의를 받아둔 경우이기 때문으로 이해된다.

금융기관이 (예외사유가 아님에도) 본인확인의무를 이행하지 않고 접근매체를 발급하였다면 어떠한 법적 효과가 발생하는가? 전자금융거래법에 의하면 이 경우 당해 금융기관은 금융감독당국으로부터 행정제재(관련 업무의 전부 또는 일부의 정지)를 받게 된다(법 제43조 제2항). 문제는 그 경우의 사법상 효력인데, 전자금융거래법에는 이에 관한 명문의 규정은 없다. 생각건대 금융기관이 전술한 바와 같은 접근매체 발급상의 주의의무를 해태하여 접근매체를 발급하였고 이로 인하여 전자금융거래가 발생하였다면 그 효과는 본인에게 귀속하지 않는다(금융기관이 책임을 부담한다)고 해석하여야 할 것이다. 전술한 바와 같이 전자금융거래에서 접근매체에 의한 전자금융거래의 법적 효과는 접근매체상의 본인에게 귀속하는 것이기 때문에, 본인확인의무를 이행하지 않은 경우에는 그와 같은 효과가 발생한다고 해석할 수 없기 때문이다.

2) 전자서명법-공인인증기관

그런데 접근매체 중 '공인인증서'의 발급에 관하여는 전자서명법에 특칙이 존재한다. 동법에 의하면 공인인증서는 공인인증기관이 발급하며 이 경우에도 공인인증기관은 공인인증서를 발급받고자 하는 자의 신원을 확인하여야 한다(동법 제15조 제1항). 이때 신원확인의 절차 및 방법 등이 문제되는데, 이에 관하여는 동법 시행규칙에 관련 규정이 존재한다(동 제6항). 즉, 공인인증기관은 공인인증서를 발급받고자 하는 자의 신원을 확인하는 때에는 직접 대면하여 주민등록증 등에 의하여 그 자의

서면동의[「전자서명법」 제2조 제3호에 따른 공인전자서명(이하 "공인전자서명"이라 한다)이 있는 전자문서에 의한 동의를 포함한다]를 얻은 경우

2. 갱신 또는 대체발급 예정일 전 6월 이내에 사용된 적이 있는 접근매체는 그 예정일부터 1월 이전에 이용자에게 발급 예정사실을 알린 후 20일 이내에 이용자로부터 이의 제기가 없는 경우

실명 및 본인 여부를 확인하여야 한다(동법 시행규칙 제13조의2 제2항). 전자금융거래에서 공인인증서의 중요성(접근매체로서 본인효과귀속성, 본인확인수단, 공인전자서명)을 고려할 때에는 본인확인절차를 명확하고 구체적으로 특정할 필요가 있다는 점에서 "대면에 의한 신원(실명 및 본인)확인"이라는 절차를 명시한 것은 바람직한 입법태도라 할 것이다. 이 규정은 2006년 7월 1일부터 시행된 동법 시행규칙의 개정에 의한 것이다(그 이전의 입법에 "직접 대면하여"라는 표현을 추가한 것이다).[20] 문제는 위 시행규칙의 개정 시에 대면에 의한 신원확인이라는 원칙에 대하여 아래와 같이 중요한 예외를 동시에 두었다는 점이다.

> **전자서명법 시행규칙 제13조의2(신원확인의 기준 및 방법)** ④공인인증기관은 「금융실명거래 및 비밀 보장에 관한 법률」 제2조 제1호 각 목에 따른 금융기관에서 실지명의가 확인된 전자금융거래 가입자가 공인인증서를 발급받으려는 경우에는 정보통신망을 통하여 신원을 확인할 수 있다. 이 경우 다음 각 호의 사항을 확인하여야 한다. 〈신설 2006.6.30〉
> 1. 전자금융거래 가입자의 계정(ID)과 그 비밀번호 또는 계좌번호와 그 비밀번호
> 2. 전자금융거래 가입자의 주민등록번호
> 3. 금융기관이 전자금융거래를 위하여 가입자에게 제공한 일회용비밀번호(보안카드의 비밀번호를 포함한다) 또는 가입자 본인만이 알 수 있는 두 가지 이상의 정보

이 규정은 금융기관에서 실명이 확인된 전자금융거래 가입자의 경우 공인인증서의 발급(재발급)시에 대면에 의한 신원확인이 필요하지 않고 "정보통신망을 통하여", 즉 비대면의 방법으로 신원(본인)확인을 할 수 있다는 예외를 규정한 것이다. 이 규정은 전자금융거래법의 시행(2007.1.1.)을 앞두고 전자금융거래의 "편의성을 높이기 위하여"[21] 둔 것이다. 이 예외규정에 의하면 전자금융거래 가입자는 계좌번

20) 이정현, "2006년 시행 전자서명법의 개정내용과 향후 과제", 정보보호 정책동향(한국정보보호진흥원)(2006년), 15면은 종래 공인인증서는 대면확인 후에 발급하는 것을 원칙으로 하고 있었으나 명문 규정이 없어 논란이 되어 왔던 것을 2006년 전자서명법 시행규칙의 개정에서 대면확인의 원칙을 명문화하여 논란을 종식시켰다고 설명하고 있다.

호와 비밀번호 및 주민등록번호, 보안카드상의 비밀번호(또는 다른 두 가지 본인에 관한 정보)만으로도 공인인증서를 발급받을 수 있게 되기 때문에 전자금융거래의 편의성 향상이라는 입법목적에는 부합된다. 그러나 이 규정은 전자금융거래에서 접근매체의 중요성(본인효과귀속성)을 고려하여 접근매체는 대면에 의한 본인확인절차를 철저히 거친 후에 발급되어야 한다는 대원칙을 생각할 때에는 대단히 위험한 발상에 의한 규정이라고 하지 않을 수 없다. 전자금융사기를 의도한 자는 몇 가지 개인정보나 금융거래정보만 확보하고 있으면 대면에 의한 본인확인을 거치지 않기 때문에 '쉽게' 공인인증서를 취득하여 소기의 목적을 달성할 수 있게 되기 때문이다. 특히 개인정보와 금융거래정보의 유출사고가 사회문제화 되고 있는 현 상황에서 이 규정이 개인정보 등의 유출을 조장하고 전자금융사기에 악용될 수 있다는 점에서 더욱 그러하다. 그런데 문제의 심각성은 이와 같은 시행규칙상의 예외규정의 존재 및 그 의의를 전자상거래나 전자금융거래 실무에 종사하는 자나 법률전문가들조차 거의 인식하지 못하고 있으며,[22] 다만 금융기관의 홈페이지 등을 확인해보면 공인인증서의 재발급이 정보통신망상에서 쉽게 이루어진다는 점만이 홍보되고 있다는 점이다.[23] 있어서는 안 될 위험한 규정이 所與의 전제로서 실무에서 활용되고 있는 비정상적인 상황을 어떻게 이해할 것인가? 만일 이와 같은 실무관행에 의해 본인이 아닌 자가 공인인증서를 재발급 받아 전자금융거래를 하였다면 그 법적 효과는 본인에게 귀속한다(본인이 책임을 져야 한다)고 하여야 할 것인가? 본 사안은 실로 이와 같은 점이 문제된 사안이라 하지 않을 수 없다.

---

21) 법제처 「전자서명법 시행규칙」 (2006.6.30. 개정) 개정이유 참조.

22) 이것은 필자가 주변의 실무가나 법률전문가 수인을 대상으로 직접 확인한 것이다.

23) 실무에서는 공인인증서의 '재발급'에 대하여, 분실이나 컴퓨터 포맷 등의 경우에 공인인증서를 재차 발급받는 것으로서 기존 인증서의 유효기간은 유지되지만 기존 인증서는 자동 폐기되는 것으로 설명하고 있다(국민은행 홈페이지 등 참조). 따라서 유효기간이 경과되기 전에 공인인증서를 '갱신'하는 것과는 구별된다. 한편 공인인증서의 발급주체는 공인인증기관이지만 실제로는 금융기관의 창구나 홈페이지에서 발급이 가능하다. 이것은 공인인증기관이 발급한 공인인증서가 금융기관을 통하여 이용자에게 제공되기 때문으로 이해된다.

(3) 접근매체의 사용 및 관리상의 주의의무–이용자

전술한 바와 같이 전자금융거래에서의 접근매체의 중요성으로부터 금융기관 (및 공인인증기관)은 그 발급상의 주의의무를 부담한다. 한편 발급된 접근매체에 대하여 이용자는 사용 및 관리상의 주의의무를 부담한다. 즉, 이용자는 접근매체를 사용 및 관리함에 있어서 ①접근매체를 양도하거나 양수하는 행위, ②대가를 주고 접근매체를 대여받거나 대가를 받고 접근매체를 대여하는 행위, ③접근매체를 질권의 목적으로 하는 행위, ④이상의 행위를 알선하는 행위를 하여서는 아니 되며(법 제6조 제3항), 이에 위반한 경우 형사벌에 처해진다(법 제49조 제4항).

한편 전자금융거래법은 접근매체의 위조나 변조로 발생한 사고로 인하여 이용자에게 손해가 발생한 경우 금융기관이 손해를 배상할 책임이 있다는 취지를 규정하면서(법 제9조 제1항) 중대한 예외를 동시에 두고 있다. 즉, 이용자가 접근매체의 사용 및 관리에 고의 또는 중대한 과실이 있는 경우 금융기관이 면책되고 이용자가 그 책임을 부담한다는 것이다(법 제9조 제2항). 이때 이용자의 고의나 중대한 과실의 범위는 다음과 같다.

> **전자금융거래법 시행령 제8조(고의나 중대한 과실의 범위)** 법 제9조제3항에 따른 고의나 중대한 과실의 범위는 다음 각 호와 같다.
> 1. 이용자가 접근매체를 제3자에게 대여하거나 그 사용을 위임한 경우 또는 양도나 담보의 목적으로 제공한 경우(법 제18조에 따라 선불전자지급수단이나 전자화폐를 양도하거나 담보로 제공한 경우를 제외한다)
> 2. 제3자가 권한 없이 이용자의 접근매체를 이용하여 전자금융거래를 할 수 있음을 알았거나 쉽게 알 수 있었음에도 불구하고 접근매체를 누설하거나 노출 또는 방치한 경우

여기서 제1호는 이용자가 (경제적 목적 등을 위하여) 스스로 접근매체의 점유 내지 지배(control)를 제3자에게 이전한 경우로서, 형사벌의 대상이 되는 접근매체의 사용 및 관리행위(법 제6조 제3항)와 대체적으로 일치한다. 이러한 경우에 이용자의 고의나 중과실을 인정하는 것은 문제가 없다고 할 것이다. 한편 제2호는 접근매체를 제3자에게 직접 이전한 것은 아니나 제3자에 의한 접근매체의 사용가능성을 제공하

였다는 점에서 고의나 중대한 과실로 인정될 수 있는 경우이다. 문제는 "제3자가 권한 없이 이용자의 접근매체를 이용하여 전자금융거래를 할 수 있음을 알았거나 쉽게 알 수 있었음에도 불구하고" 접근매체를 누설 등 하였다는 한정이 붙는다는 점이다. 즉, 그와 같은 경우에 한하여 접근매체의 누설 등의 사용이나 관리행위에 대하여 이용자가 책임을 부담한다는 것이다. 따라서 이용자가 접근매체를 누설 등 하였으나 제3자가 무권한거래를 할 수 있음을 '쉽게' 알 수 없었던 경우에는 금융기관은 면책되지 않는다고 해석할 것이다. 여기서 이용자가 '쉽게 알 수 있었는지의 여부'(이것이 곧 중과실 판단의 핵심적 관건이 될 것이다)는 이용자측 사정(직업이나 금융거래 경력 등)뿐만 아니라 제3자의 기망행위의 정도 및 금융기관의 정보보안 실태 등을 종합적으로 고려하여 판단하여야 할 것이다. 제3자의 기망행위의 정도가 강하거나 금융기관의 정보보안이 취약한 상황에서라면 이용자에게 책임을 부담시킬 수는 없다고 판단되기 때문이다. 특히 정보보안이 취약하다는 것은 시스템거래로서의 전자금융거래 자체의 안전성이 취약하다는 것을 의미하기 때문에 이로 인한 책임을 이용자에게 전가하는 해석론은 타당하다고 할 수 없다. 따라서 예컨대 전술한 바와 같이 공인인증서의 발급이 정보통신망상에서 쉽게 이루어질 수 있는 상황, 즉 정보보안이 허술한 상황에서라면 이용자의 중과실 판단은 신중하게 이루어져야 할 것이다.

IV. 본 판결의 검토

전자금융거래법에서 접근매체를 이와 같이 이해할 경우, 본 사안에서 원심 및 대법원의 판결은 특히 다음과 같은 점에서 문제가 있다고 할 것이다.

1. 금융거래정보 등의 노출을 접근매체의 노출과 동일시할 수 있는가?

(1) 원심 및 대법원은 본 사안의 원고가 "제3자에게 접근매체인 공인인증서의

발급에 필수적인 계좌번호, 계좌비밀번호, 주민등록번호, 보안카드번호, 보안카드비밀번호를 모두 알려준 점 등에 비추어 보면, 원고가 제3자가 권한 없이 접근매체를 이용하여 전자금융거래를 할 수 있음을 알았거나 쉽게 알 수 있었음에도 이를 노출하였다고 볼 것"이고 따라서 원고에게 중과실이 인정된다고 판시하고 있다. 이러한 판단은 원고가 노출한 금융거래정보가 공인인증서 발급에 필수적인 정보라는 점에서, 금융거래정보를 접근매체와 동일시하는 생각에 기초해 있다.

(2) 그러나 이러한 생각에는 찬동하기 어렵다. 그 이유는 다음과 같다.

첫째, 접근매체의 개념표지(세 가지 기능)를 명시하고 그 종류를 다섯 가지로 한정열거함과 동시에, 이용자의 중과실의 범위에 관해서도 이를 접근매체의 (점유 내지 지배의) 이전이나 사용가능성의 제공으로 엄격하게 한정하고 있는 전자금융거래법의 명시적 태도에 반한다. 대법원과 같이 "금융거래정보=접근매체"와 같이 해석한다면 전자금융거래법이 '접근매체'라는 개념을 통하여 시스템거래로서의 전자금융거래의 기술적 구조를 설명하고자 한 근본적인 생각 및 법체계 전체가 흔들릴 수밖에 없다.[24] 따라서 접근매체를 다섯 가지로 한정열거하고 이용자의 중과실의 범위에 관하여도 이를 '접근매체'의 이전이나 사용가능성의 제공으로 한정하고 있는 입법태도를 바꾸지 않는 한, 원고가 접근매체를 노출하지 않았음에도 불구하고 이로부터 원고의 중과실을 이끌어내는 해석은 법률의 문리적 해석 범위를 넘는 것이라 하지 않을 수 없다.

둘째, 그럼에도 불구하고 원고가 '보안카드번호 및 보안카드비밀번호'를 노출하였다는 것은 중과실로 판단될 여지가 있다. 이들은 공인인증서를 통하여 시스템에 접근한 이용자가 최종적으로 거래지시를 하는데 필요한 보안수단으로서 공인인증서와 함

24) 전술한 바와 같이 현행법상 '금융거래정보'로서 정의된 접근매체는 ③이용자번호 및 ⑤(전자식 카드나 공인인증서를 사용하는데 필요한) 비밀번호에 한정된다. 그러나 이들은 현재의 실무상으로는 단독으로는 시스템에의 접근을 가능하게 하지 못하고 다만 다른 수단과 함께 또는 보조적으로 사용되는 접근매체일 뿐이다.

께 실무상 중요하게 활용되고 있기 때문이다. 그러나 보안카드 관련정보도 (당시의) 현행법상으로는 '접근매체'로 정의되어 있지 않고 다만 실무상으로만 활용되는 보안수단이라는 점에서 이를 또한 접근매체의 노출과 동일시 할 수는 없고, 따라서 그 노출로부터 이용자의 중과실을 이끌어내는 해석에는 역시 찬성하기 어렵다.

이와 관련하여 금융기관의 책임범위 및 이용자의 중과실의 범위를 확장한 최근의 전자금융거래법 및 동법 시행령의 개정(양자 모두 2013.11.23. 시행)이 주목된다.[25] 즉, 이 개정으로 접근매체의 위조나 변조로 발생한 사고뿐만 아니라 "전자적 장치나 정보통신망에 침입하여 거짓이나 그 밖의 부정한 방법으로 획득한 접근매체의 이용으로 발생한 사고"로 인하여 이용자에게 발생한 손해는 원칙적으로 금융기관이 배상책임을 부담하지만(법 제9조 제1항 제3호),[26] 금융기관이 보안강화를 위하여 전자금융거래 시 요구하는 추가적인 보안조치를 이용자가 정당한 사유 없이 거부하거나, 추가적인 보안조치에 사용되는 매체·수단 또는 정보에 대하여 이용자가 이를 노출 등을 하거나 양도 또는 담보제공 등을 하여 위 (추가된) 사고가 발생한 경우에는 이용자의 중과실로 판단되어 금융기관이 면책된다는 점이 추가되었다(법 시행령 제8조 제3호·제4호).[27] 이 개정은 (시기적으로도 내용적으로도) 실로 본 사안의 쟁점을

25) 전자금융거래법(법률 제11814호, 2013.5.22., 일부개정, 동년 11.23. 시행), 동법 시행령(대통령령 제24880호, 2013.11.22., 일부개정, 동년 11.23. 시행).

26) **법 제9조(금융회사 또는 전자금융업자의 책임)** ① 금융회사 또는 전자금융업자는 다음 각 호의 어느 하나에 해당하는 사고로 인하여 이용자에게 손해가 발생한 경우에는 그 손해를 배상할 책임을 진다. 〈개정 2013.5.22.〉

1. 접근매체의 위조나 변조로 발생한 사고
2. 계약체결 또는 거래지시의 전자적 전송이나 처리 과정에서 발생한 사고
3. 전자금융거래를 위한 전자적 장치 또는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호에 따른 정보통신망에 침입하여 거짓이나 그 밖의 부정한 방법으로 획득한 접근매체의 이용으로 발생한 사고 (*하선이 추가된 부분임)

27) **법 시행령 제8조(고의나 중대한 과실의 범위)** 법 제9조제3항에 따른 고의나 중대한 과실의 범위는 다음 각 호와 같다 〈개정 2013.11.22.〉

1. 이용자가 접근매체를 제3자에게 대여하거나 그 사용을 위임한 경우 또는 양도나 담보의 목적으로 제공한 경우(법 제18조에 따라 선불전자지급수단이나 전자화폐를 양도하거나 담보로 제공한 경우를 제외한다)

입법화한 것으로 보이는데, 후술하는 바와 같이 성명불상자는 정보통신망에 침입하여 거짓이나 그 밖의 부정한 방법으로 접근매체를 재발급받아 이를 이용하여 전자금융사고를 일으켰고, 본 사안의 원고는 "보안강화를 위하여 전자금융거래 시 요구하는 추가적인 보안조치"인 보안카드 관련정보를 노출하였다고 할 것이다. 따라서 개정법의 내용대로라면 본 사안에서 원고의 보안카드 관련정보 노출행위는 위 중과실의 범위에 포섭되게 될 것이다. 그렇다면 이 개정법이 시행되기 이전에 발생한 본 사안의 경우에도 개정법과 같이 해석하여야 할 것인가? 생각건대 "보안강화를 위하여 전자금융거래 시 요구하는 추가적인 보안조치"(본 사안에서는 보안카드)를 접근매체와는 구별하여 규정하고 있는 개정법의 입법태도로 볼 때 '보안카드 관련정보'를 '접근매체'와 동일시할 수 없다는 것은 이 개정법으로부터도 분명해졌다. 따라서 보안카드 관련정보를 노출한 본 사안을 접근매체의 노출과 동일시하는 원심 및 대법원의 해석은 (당시의) 전자금융거래법의 문리적 해석범위를 넘는 것이라고 하지 않을 수 없다. 그런 점에서 본 판결은 말하자면 '입법의 불비'라는 리스크를 이용자에게 고스란히 떠넘긴 판결이라고도 볼 수 있을 것이다.

(3) 그렇다면 본 사안은 접근매체가 노출된 사안이 아니라 다만 금융거래정보 및 추가적 보안조치에 사용되는 정보(보안카드 관련정보)가 노출된 사안이라고 파악하여야 할 것이고, 따라서 접근매체(공인인증서)의 발급에 필수적이라는 이유로 이

---

2. 제3자가 권한 없이 이용자의 접근매체를 이용하여 전자금융거래를 할 수 있음을 알았거나 쉽게 알 수 있었음에도 불구하고 접근매체를 누설하거나 노출 또는 방치한 경우
3. 금융회사 또는 전자금융업자가 법 제6조제1항에 따른 확인 외에 보안강화를 위하여 전자금융거래 시 요구하는 추가적인 보안조치를 이용자가 정당한 사유 없이 거부하여 법 제9조제1항제3호에 따른 사고가 발생한 경우
4. 이용자가 제3호에 따른 추가적인 보안조치에 사용되는 매체·수단 또는 정보에 대하여 다음 각 목의 어느 하나에 해당하는 행위를 하여 법 제9조제1항제3호에 따른 사고가 발생한 경우
가. 누설·노출 또는 방치한 행위
나. 제3자에게 대여하거나 그 사용을 위임한 행위 또는 양도나 담보의 목적으로 제공한 행위
(*하선이 추가된 부분임)

들 정보를 접근매체와 동일시하여 이용자의 중과실을 이끌어낼 수는 없다고 할 것이다. 결국 이 사건 금융사고는 노출된 금융거래정보 및 보안카드 관련정보를 이용하여 (이용자의 의사에 반하여) 접근매체를 발급받은 것이기 때문에 "접근매체의 위조로 발생한 사고"(법 제9조 제1항 제1호)라 할 것이고, 개정법하에서는 "시스템에 침입하여 거짓이나 그 밖의 부정한 방법으로 획득[재발급]한 접근매체의 이용으로 발생한 사고"(개정법 제9조 제1항 제3호)라고 이해할 것이다.

2. 성명불상자의 기망행위의 평가

(1) 원심 및 대법원의 판결은 성명불상자에 의한 기망행위에 대한 법적 평가가 누락되어 있는 점에서 문제이다. 본 사안에서 원고가 금융거래정보 등을 노출한 것은 제3자(성명불상자)가 이른바 보이스피싱 등의 사기수법에 의해 원고를 기망했기 때문이다. 그렇다면 제3자의 이와 같은 행위가 이용자의 중과실 판단에 고려되어야 할 것이다. 이점과 관련하여 대법원은 "'고의 또는 중대한 과실'이 있는지 여부는 접근매체의 위조 등 금융사고가 일어난 구체적인 경위, 그 위조 등 수법의 내용 및 그 수법에 대한 일반인의 인식 정도, 금융거래 이용자의 직업 및 금융거래 이용경력 기타 제반 사정을 고려하여 판단할 것이다"라고 하여 "접근매체의 위조 등 금융사고가 일어난 구체적인 경위, 그 위조 등 수법의 내용"(하선부분)을 판단기준으로 들고 있다. 따라서 적어도 대법원으로서는 제3자의 기망행위에 관한 평가가 이용자의 중과실 판단에 고려되어야 함을 일반론으로서 설시한 것으로 이해할 것이다. 그럼에도 불구하고 대법원이 원고에게 중과실이 있다고 판단한 이유는, "그 수법에 대한 일반인의 인식 정도, 금융거래 이용자의 직업 및 금융거래 이용경력"을 더 고려했기 때문이라고 이해된다. 즉, ① 이 사건 금융사고 당시에는 이른바 전화금융사기가 빈발하여 이에 대한 사회적인 경각심이 높아진 상태였던 점, ② 원고는 이 사건 금융사고 당시 만 33세로서 공부방을 운영하는 등 사회경험이 있었고 1년 이상 인터넷뱅킹을 사용해왔던 점, ③ 원고는 관련 형사 사건의 조사과정에서 성명불상자로부터 '001'로 시작되

는 국제전화를 받아 순간 이상하다는 생각을 하였다고 진술하고 있는 점으로부터 원고의 중과실을 이끌고 있는 원심의 판단을 정당하다고 평가하고 있기 때문이다.

(2) 생각건대 원심과 대법원이 위와 같은 이유로 원고의 중과실을 인정한 것은 전자금융사기 수법을 지나치게 경시하였거나 이용자의 주관적 요소를 과도하게 높게 평가한 때문이라고 생각된다. 전자금융사기 수법은 "허물을 벗는 파충류처럼 변태를 거듭하고 있다."[28] 자녀의 전화번호로 연락해 (다른 이의) 비명 소리를 들려주고 당장 돈을 부치지 않으면 죽이겠다고 (거짓으로) 협박하는 고전적인 수법에서부터 이용자의 PC나 스마트폰 등에 악성코드를 심어 가짜 사이트로 유도한 후 정보를 입력하게 하는 고도의 기술적 수법 등 전자금융사기의 수법은 실로 다양하고 날로 진화하고 있다.[29] 그 중에서 본 사안에서는 이른바 보이스피싱(voice phishing)과 피싱(phishing)이라는 사기수법이 함께 사용된 것으로 보인다. 전자는 전화를 통하여 피해자로 하여금 신용카드 비밀번호 등의 진술을 유도하거나 피해자를 ATM으로 유도하여 자금을 직접 이체시키는 사기수법이고, 후자는 이메일을 발송하여 이메일에서 안내하는 가짜 사이트에 접속하게 하여 비밀번호 등의 입력을 유도하는 사기수법이다. 본 사안에서 성명불상자는 이 두 가지를 교묘하게 섞어 원고의 금융거래정보 등을 노출케 하였다. 즉 성명불상자는 우선 자기를 검사라 사칭하였고 원고가 전자금융사기 범죄의 공범이 아닌지 확인이 필요하다고 하여 불안감을 조성한 후 가짜 대검찰청 사이트로 유도하여 원고의 금융거래정보와 보안카드 관련정보를 입력하게 하였다.

그러나 이와 같은 사실관계에 대하여 원심과 대법원은 "전화금융사기가 빈발하여 이에 대한 사회적인 경각심이 높아진 상태였던 점"을 "그 수법에 대한 일반인의 인

28) 조선닷컴, 2013.1.30. 기사, "[신용사회의 敵들] [7] 해외 거래까지 콕 찍어 정밀 해킹..거액 송금 낚아채"

29) 현재까지 등장한 전자금융사기 수법에는 보이스피싱(voice phishing), 스미싱(smishing), 파밍(pharming), 메모리해킹(memory hacking), 메신저 피싱(messenger phishing) 등이 있고 계속 새로운 유형이 발생하고 있다.

식정도"로 파악하여 원고의 중과실 인정의 하나의 유력한 근거로 들고 있다. 그런데 원심과 대법원의 판단대로라면 전화금융사기는 사회적 경각심 내지 인식이 높아진 상태였기 때문에 그 발생건수나 피해액수가 소소한 정도에 머물러 있어야 할 터이다. 그러나 비교적 고전적 사기수법이라 할 만한 보이스피싱에 의한 피해의 실태조차도 원심과 대법원이 생각하는 만큼 그리 간단하지 않다. 경찰청의 통계에 의하면 2013년 1월~10월까지의 보이스피싱에 의한 피해건수는 4,022건이고, 피해액은 436억원에 이른다.[30]

대법원이 설시하듯 "금융거래 이용자의 직업 및 금융거래 이용경력"을 고려하여 이용자의 중과실을 판단하는 것은 필요하다. 그러나 전자금융거래의 세계에서는 이것이 절대적이거나 유력한 기준이 될 수는 없다고 생각한다. 이 기준은 전자금융사기 수법이 어떠한지에 관한 판단과 함께 고려되어야 한다. 전술한 바와 같이 본 사안에서는 두 가지 전자금융사기 수법을 교묘히 섞었다는 점, 검사를 사칭하고 원고가 전자금융사기 범죄의 공범이라고 불안감을 조성하였다는 점, 가짜 대검찰청 사이트를 만들어 금융거래정보 등을 입력하도록 이용자를 유도하는 등 일련의 과정이 고도의 계산된 수법에 따라 일관되게 이루어졌고 기술적으로 이를 뒷받침하였다는 점 등에 기망행위로서의 특징이 있다. 따라서 아무리 사회경험이 있고 인터넷뱅킹의 경험이 있는 자라 하더라도 위와 같은 사기수법 하에서라면 검사사칭자의 지시대로 움직일 수밖에 없는 개연성을 갖고 있다고 생각한다.[31] 그렇다면 원고의 행위에 과실이 있다는 점은 인정할 수 있다 하더라도, 그것이 '중과실'로까지 평가될 수 있는지는 의문이다.

(3) 비교법적으로는 전자금융거래에서 제3자에 의한 무권한거래가 발생한 경우,

30) 위 조선닷컴 기사의 '사이버범죄수사대'(경찰청 사이버테러 대응센터)의 통계자료를 참조.

31) 머니투데이, 2014.04.14. 기사, "신종 수법에… 경찰학과 교수, 보이스피싱으로 5천만원 피해"에 의하면 정보보안 전문가인 한 경찰행정학과 교수가 본 사안과 거의 유사한 사기 수법으로(이른바 파밍 수법이 추가되었다) 5000만원의 피해를 입었다고 한다.

피해자의 중과실을 요건으로 하여 금융기관을 면책시키는 입법례로서 일본의 「예금자보호법(2005)」[32]을 들 수 있다. 이법은 현금카드나 (ATM거래가 가능한) 통장(이하 양자를 합쳐 '카드등'이라 한다)에 의한 ATM거래가 대단히 발달한 일본 사회에서 2000년대 이후 카드등의 위조나 도난에 의한 무권한거래가 급증함에 따라 그 피해자를 보호하기 위한 목적에서 제정된 것이다.[33] 이법은 예금의 지급이 위조된 현금카드나 통장(이하 "위조카드등"이라 한다)을 이용하여 이루어진 경우에는 일본 민법 제478조(한국민법 제470조)에 의한 '채권의 준점유자변제' 법리의 적용을 배제하여 당해 변제의 예금자에 대한 효과귀속을 부정(=무효화)하면서(3조), 다만 이 경우 금융기관이 면책되는 경우를 다음의 두 경우로 한정한다(4조). 즉, ①예금자가 고의로 위조카드등에 의한 거래가 일어나도록 한 경우나, ②금융기관이 선의무과실이고 예금자의 중대한 과실로 위조카드등에 의한 거래가 일어난 경우가 그것이다. 또한 카드등의 도난으로 의해 무권한거래가 일어난 경우에는 예금자가 일정한 절차적 요건(신속한 사고통지 등)을 충족하면 예금자에게 손해전보청구권을 인정한다. 다만 이 경우 금융기관이 예금자의 경과실을 입증하면 전보액은 3/4으로 감액되며, 금융기관이 예금자의 중과실을 입증하면 전액 면제되도록 하고 있다(5조). 요컨대 위조카드에 의한 무권한거래가 예금자의 중과실로 발생할 경우에는 금융기관은 면책(예금자에게 당해 거래의 효과가 귀속)되고, 도난 카드등에 의한 무권한거래에서 예금자에게 중과실이 있는 경우 예금자에게 손해전보청구권은 발생하지 않는다.

결국 이법에 의하면 예금자에게 중과실이 있는 경우에는 위조나 도난에 의한 무권

32) 정식명칭은 "偽造カード等及び盗難カード等を用いて行われる不正な機械式預貯金払戻し等からの預貯金者の保護等に関する法律"(위조카드등 및 도난카드등을 이용하여 이루어진 부정한 기계식예저금의 인출등으로부터의 예저금자의 보호등에 관한 법률)이다.

33) 이법에 관한 일본어 문헌으로서 우선, 高見澤昭治・齋藤雅弘・野間啓 編著『預金者保護法ハンドブック』(日本評論社、2006) ; 松本恒雄「預金者保護に向けた法整備と残された課題」自由と正義57巻3号(2006.3) 54頁以下를 참조. 한편, 서희석, "훔친 통장과 인장을 이용한 예금인출의 유효성-대법원 2007.10.25. 선고 2006다44791 판결에 대한 비판적 검토-", 소비자문제연구 제35호(2009.4) 60면 이하에서도 이법을 간단히 소개하고 있다.

한거래로부터 예금자는 보호받지 못하기 때문에 예금자의 '중과실'의 범위가 문제된다. 이에 관하여 명문의 규정은 없으나, 법안제출자는 "고의와 동일시할 수 있을 정도로 주의의무에 현저한 위반이 있는 경우"를 중과실로 설명하면서, 구체적인 예로서 다음의 세 가지를 예시하고 있다. 즉, ①타인에게 비밀번호를 알린 경우, ②비밀번호를 카드등 위에 기록한 경우, ③예금자가 스스로 카드등을 안이하게 제3자에게 넘긴 경우가 그것으로서, 이와 같은 경우에는 예금자의 중과실이 인정된다는 것이다.[34] 이것은 우리의 전자금융거래법상의 이용자의 중과실의 범위와 대체로 같은 발상에 의한 것으로 이해된다. 그런데 주의할 점은 ①의 경우 "제3자의 기망행위가 개입되어" 예금자가 타인에게 비밀번호를 알린 경우에도 중과실로 인정할 것인지에 대하여 일본 내에서는 다음과 같은 해석론이 전개되고 있다는 사실이다. 즉, "예컨대 제3자가 은행이나 경찰 등을 사칭하여 예금자에게 전화를 걸은 후 '확인을 위해 비밀번호를 알려달라'는 등으로 예금자를 기망하여 비밀번호를 알아차리게 된 경우에는 예금자에게 중과실이 있다고는 해석되지 않는다"는 것이다. "속아서 비밀번호를 알린 경우가 '고의와 동일시할 정도로' 현저한 주의의무 위반이 인정되는 경우라고는 도저히 평가되지 않기 때문"이다."[35][36]

중과실의 범위에 관한 이와 같은 해석론은 우리법상 본 사안에서와 같이 제3자의 기망행위에 의해 금융거래정보가 노출된 경우에도 마찬가지로 타당한 것이라고 생각된다. 제3자가 기망행위를 통하여 이용자로 하여금 금융거래정보를 노출하게 하였다면 이용자에게 고의와 동일시할 정도의 현저한 주의의무 위반이 있다고는 '도저히' 평가되지 않기 때문이다.

---

34) 高見澤昭治 외, 앞의 문헌, 61면.

35) 高見澤昭治 외, 앞의 문헌, 61~62면.

36) 일본의 예금자보호법은 원래는 ATM 등에 의한 기계식인출거래를 대상으로 하기 때문에 인터넷뱅킹에는 적용이 없다. 그러나, 동법의 제정 후 은행업계가 자발적으로 인터넷뱅킹의 경우에도 위 법에 준하여 은행별로 개별적으로 대응한다는 자주대응책을 공표하였다(2008년 2월 10일). 따라서 인터넷뱅킹의 경우에도 위와 같은 해석론이 기본적으로는 그대로 타당하다고 생각된다(서희석, 앞의 논문, 61면 참조).

(4) 한편 우리의 대법원 판결례 중에는 착오취소가 문제된 사안에서 상대방이 사회적으로 높은 지위에 있는 자의 자격을 (묵시적으로) 사칭한 사안[37]이나, 상대방에 의해 유발된 동기의 착오의 사안[38]에서 착오자의 '중과실'을 인정하지 않은 사례가 있다. 앞의 사안의 경우 "일반인의 입장에서는 그에게 당연히 [그와 같은] 자격이 있는 것으로 믿을 수밖에 없었을 것"이라는 점이, 뒤의 사안에서는 "매도인의 적극적인 행위에 의하여 매수인이 착오에 빠진 점"이 각각 표의자의 중과실을 부정하는 근거로 사용되었다. 본 사안은 착오취소의 사안은 아니지만 착오자의 중과실(민법 제109조 제1항 단서) 판단에 위와 같은 점들이 고려되고 있다는 점은 참조할 수 있다고 생각한다.

3. 공인인증서 재발급의 법적 함의

(1) 원심 및 대법원의 판단 중에서 가장 이해할 수 없는 점은 본 사안에서 금융거래정보 및 보안카드 관련정보의 노출이 어떻게 공인인증서의 재발급으로 연결될 수 있는지에 관하여 아무런 언급이 없고 다만 이를 所與의 전제로 삼고 있다는 점이다. 전술한 바와 같이 시스템거래로서의 전자금융거래에서 접근매체의 중요성(본인효과 귀속성)으로부터 그 발급은 대면에 의한 본인확인을 거쳐 철저하게 이루어져야 함에

37) 예컨대, **대법원 2003.4.11.선고 2002다70884 판결**(설계용역계약 체결을 전후하여 건축사 자격이 없다는 것을 묵비한 채 자신이 미국에서 공부한 건축학교수이고 '○○건축연구소'라는 상호로 사업자등록까지 마치고 건축설계업을 하며 상당한 실적까지 올린 사람이라고 소개한 경우, 일반인의 입장에서는 그에게 당연히 건축사 자격이 있는 것으로 믿을 수밖에 없었을 것이므로, 재건축조합 측이 그를 무자격자로 의심하여 건축사자격증의 제시를 요구한다거나 건축사단체에 자격 유무를 조회하여 이를 확인하여야 할 주의의무가 있다고 볼 수는 없다고 보아 재건축조합의 착오가 중대한 과실로 인한 것이 아니라고 한 사례).

38) 예컨대, **대법원 1997.9.30.선고 97다26210 판결**(매도인의 적극적인 행위에 의하여 매수인이 착오에 빠지게 된 점, 매수인이 그 건물의 일부가 철거되지 아니할 것이라고 믿게 된 경위 등 제반 사정에 비추어 보면 착오가 매수인의 중대한 과실에 기인한 것이라고 할 수 없다고 한 사례).

도 불구하고 원심 및 대법원의 판결에는 이에 관한 판단이 전혀 없기 때문이다. 그러나 전술한 바와 같이 공인인증서의 발급절차로서 정보통신망을 통하여 비대면의 방법으로 본인확인을 거치도록 허용하는 전자서명법 시행규칙의 개정(2006년)에 따라 몇 가지 금융거래정보만으로도 정보통신망 상에서 공인인증서를 쉽게 발급할 수 있게 되었다. 따라서 '금융거래정보'의 노출을 '접근매체'의 노출과 동일시하는 원심 및 대법원의 판단은 이와 같은 입법 및 실무관행을 전제로 한 것이라고 선해할 수는 있을 것이다. 문제는 이와 같은 입법 및 실무관행을 전제로 할 경우 전자금융거래의 보안수준에는 심각한 문제가 발생한다는 점이다. 즉 현행 전자금융거래에서 (예금인출거래가 아닌 한) 가장 중요한 접근매체인 공인인증서의 (재)발급이 대면에 의한 본인확인 절차 없이도 정보통신망 상에서 쉽게 이루어지고 따라서 이를 악용한 전자금융사기가 발생한다면 그 책임은 누구에게 물어야 할 것인가가 문제되는 것이다.

(2) 이점과 관련하여 원고는 피고은행에 설사 전자금융거래법 제9조 제1항의 책임이 인정되지 않는다 하더라도 피고은행이 원고에게 공인인증서 재발급 사실을 통지하여야 할 주의의무가 있으나 이를 게을리하여 결국 이 사건 금융사고를 방지하지 못하고 원고에게 손해를 입혔으므로 과실에 의한 불법행위방조책임이 성립한다고 주장하였고, 원심과 대법원은 이에 대해 피고은행에게 그와 같은 통지의무가 존재한다고 보기 어렵고, 원고가 문자메시스 서비스를 신청하지도 않았으며, 설령 피고들에게 통지의무가 있다고 하더라도 이를 이행하지 않음으로써 이 사건 금융사고가 발생하였다고 단정하기도 어렵다는 점을 들어 원고의 주장을 배척하고 있다.

생각건대 현행 전자서명법 시행규칙 상의 공인인증서 발급절차대로라면 극단적인 경우 공인인증서는 계좌번호와 비밀번호, 주민등록번호 및 보안카드의 비밀번호만 알면 재발급이 가능하게 된다. 결국 이들 정보만으로 공인인증서의 재발급이 가능한 상황이라면 (개인정보 및 금융거래정보의 유출이 사회문제화 되고 있는 현 상황에서는 더더욱) "보안카드의 비밀번호"가 이용자가 의존할 수 있는 유일한 보안수단이 되는 셈이다.[39] "전자금융거래의 안전성 확보"를 최고의 이념으로 삼는 전자금융거래법의 입법취지(법 제1조 참조)를 고려할 때 이와 같은 상황은 결코 바람직스러운

것이라 할 수 없다.

그렇다면 이와 같이 전자금융거래의 정보보안 수준이 취약한 상황에서 금융기관은 전자금융거래의 안전성 확보를 위하여 어떠한 주의의무를 부담한다고 해석하여야 할 것인가? 장래적으로 가장 바람직한 것은 대면에 의한 공인인증서의 발급절차에 중요한 예외를 인정한 전자서명법 시행규칙의 관련규정을 삭제하거나 개선하여 공인인증서의 발급이 보다 엄격하게 이루어지도록 하는 것이다. 그러나 그것은 입법자의 몫이기 때문에 그것이 실현되지 않은 현 상황에서 금융기관에게 입법을 촉구하거나 다른 보안수단의 개발을 강요할 수는 없다. 그러나 공인인증서 재발급 절차의 허술함을 알고 있거나 (백보 양보하여) 최소한 알고 있어야 할 금융기관의 입장에서는 이용자에게 공인인증서의 재발급으로 인하여 피해가 발생하는 것은 막아야 할 주의의무가 발생한다고 해석할 수는 있을 것이다. 그 근거는 전자금융거래의 안전성의 확보를 이념으로 하는 전자금융거래법의 입법목적(제1조) 및 이를 명문화한 동법 제21조(안전성의 확보의무)[40]에서 찾을 수 있을 것이고, 궁극적으로는 신의칙을 근거로 할 수 있을 것이다.

(3) 이와 같은 해석을 전제로 한다면 전자금융거래 이용자의 중과실 판단에 관한 기준으로서 "금융기관의 전반적인 정보보안 수준"이 누락된 것은 아쉬운 점이다. 만일 이와 같은 판단기준이 포함되었다면 본 사안과 같이 금융기관의 정보보안이 취약한 상황하에서라면 이용자의 중과실 판단은 보다 신중하게 이루어졌을 것이기 때문이다. 그러나 설사 위와 같이 해석할 수 없다 하더라도 최소한 피고은행이 원고에게 공인인증서 재발급 사실을 통지하여야 할 주의의무가 있다는 원고의 주장(예비적 청구)에는 설득력이 있다고 할 것이다. 따라서 통지서비스를 원고가 신청하지 않았기 때문에 통지의무가 발생하지 않는다는 원심과 대법원의 판단은 전술한 바와 같은 공

39) 최근에 일부 금융기관이 OTP(One Time Password) 등 새로운 보안수단의 발급에 힘을 쏟는 것은 이와 같은 상황을 인식했기 때문으로 이해된다.

40) **법 제21조(안전성의 확보의무)** ① 금융기관·전자금융업자 및 전자금융보조업자는 전자금융거래가 안전하게 처리될 수 있도록 선량한 관리자로서의 주의를 다하여야 한다.

인인증서 발급절차 상의 문제점을 인식하지 못하고 전자금융거래에서 금융기관의 안전성 확보의무를 지나치게 좁게 해석하였다는 점에서 비판을 면할 수 없을 것이다. 또한 원심과 대법원은 피고은행에게 통지의무가 있다고 하더라도 이를 이행하지 않음으로써 이 사건 금융사고가 발생하였다고 단정하기도 어렵다고 판시하고 있으나 이점도 수긍하기 어렵다. 만일 공인인증서 재발급이 이루어진 그 시점에 피고은행이 원고에게 그 사실을 통지하였다면, 원고의 조치에 따라서는 시간적으로도 그 이후의 금융사고를 막을 개연성은 충분히 있었다고 판단되기 때문이다.

V. 본 판결의 의의 및 평가

1. 본 판결의 의의

본 판결은 보이스피싱 등 전자금융사기로 인한 전자금융거래 이용자의 손해에 대한 금융기관의 법적 책임이 문제된 최초의 대법원 판결이라는 점에서 중요한 의의를 갖는다. 본 판결에 따라 향후에 이용자의 중과실을 판단할 경우에는 "접근매체의 위조 등 금융사고가 일어난 구체적인 경위, 그 위조 등 수법의 내용 및 그 수법에 대한 일반인의 인식 정도, 금융거래 이용자의 직업 및 금융거래 이용경력 기타 제반 사정을 고려하여 판단"하게 될 것이고, 특히 사회적으로 널리 알려진 전자금융사기에 의해 이용자가 금융거래정보 등을 노출하였고 이로 인해 손해를 입은 경우에는 중과실로 판단될 가능성이 크게 되었다고 할 것이다. 따라서 이 판결로 향후에 전자금융거래에서의 이용자의 주의의무가 더욱 '엄격하게' 요구되게 되었다고 할 것이다. 한편 실질적인 본법의 쟁점(보안카드 관련정보 노출의 중과실 여부)은 (본 대법원 판결이 선고되기도 전에) 전술한 바와 같이 전자금융거래법의 개정으로 동법에 반영되었기 때문에 향후에는 이 개정법에 따라 처리하게 될 것이다. 다만 이용자가 "추가적인 보안조치에 사용되는 매체·수단 또는 정보"가 아니라 (그밖에 다른) '금융거래정보'를 노출하였다면 본 판결이 선례로서 기능할 가능성은 있다고 할 것이다. 그러나 사

견으로서는 후술하는 바와 같이 본 판결에 반대하기 때문에 본 판결의 사정범위는 될 수 있는 한 제한적으로 해석하는 것이 타당하다고 생각한다.

2. 본 판결의 평가

본문에서 상세히 검토한 바와 같이 본 사안에서 이용자에게 중과실이 있다고 보아 금융기관의 면책을 인정한 대법원의 판단에 찬성할 수 없다. 그 이유를 간단히 요약하면 다음과 같다.

첫째, 본 판결은 금융거래정보가 공인인증서 발급에 필수적이라는 이유로 원고의 금융거래정보 노출을 접근매체의 노출과 동일시하고 있으나 이것은 전자금융거래법의 문리적 해석범위를 넘는 것이다. 동법은 '접근매체'의 개념표지(세 가지 기능)를 설정하고 그 종류를 다섯 가지로 한정열거하고 있을 뿐만 아니라, (당시) 이용자의 중과실의 범위도 '접근매체'를 이전하거나 노출하는 행위 등으로 한정하고 있었다. 따라서 금융거래정보가 설사 접근매체의 발급에 활용되었다 하더라도 양자를 동일시하는 해석은 동법의 해석론의 한계를 넘는 것이라고 하지 않을 수 없다.

둘째, 본 판결은 이용자의 중과실 판단에서 금융사고의 경위, 전자금융사기의 수법의 내용, 그 수법에 대한 일반적인 인식 정도, 이용자의 직업이나 금융거래 경력 등을 고려하여 판단하여야 한다고 일반론을 설시하면서도, 실제의 판단에서는 이용자 측의 사정(직업, 금융거래 경력 등)은 구체적으로 고려하고 있는 반면 금융사고의 경위 내지 전자금융사기의 수법은 구체적으로 고려하지 않고 다만 "당시 전화금융사기가 빈발하여 이에 대한 사회적인 경각심이 높아진 상태였다는 점"을 들어 원고의 중과실 인정의 하나의 중요한 근거로 삼고 있을 뿐이다. 그러나 이것은 전자금융사기 수법을 지나치게 경시한 때문이라고 생각된다. 본 사안에서 제3자(성명불상자)의 기망행위는 보이스피싱과 피싱이라는 두 가지 전자금융사기 수법을 교묘히 섞었다는 점, 검사를 사칭하고 원고가 전자금융사기 범죄의 공범이 아닌지 확인이 필요하다면서 원고를 불안하게 한 점, 가짜 대검찰청 사이트를 만들어 금융거래정보 등을 입력하도록 이용자를 유도하는 등 일련의 과정이 고도의 계산된 수법에 따라 일관되

게 이루어졌고 기술적으로 이를 뒷받침하였다는 점 등에 특징이 있다. 따라서 아무리 직업이 있고 인터넷뱅킹의 경험이 있는 자라 하더라도 위와 같은 사기수법 하에서라면 검사사칭자의 지시대로 움직일 수도 있다는 점을 고려하였어야 한다고 생각한다. 결국 이와 같은 점들을 고려하였다면 원고의 행위를 '중과실'로 평가할 수는 없었을 것이라고 생각한다.

셋째, 정보통신망을 통한 비대면의 공인인증서 발급을 허용하고 있는 현행 법제 하에서는 전자금융거래의 보안수준은 대단히 취약한 상황이라고 하지 않을 수 없다. 이와 같은 상황에서라면 금융기관의 보안수준이 이용자의 중과실 판단에도 고려되는 것이 타당하다고 할 것이고, 최소한 금융기관에게는 이용자에게 공인인증서의 재발급으로 인하여 손해가 발생하지 않도록 주의를 촉구할 의무가 발생한다고 해석할 것이다. 따라서 통지서비스를 원고가 신청하지 않았기 때문에 공인인증서 재발급 사실의 통지의무가 발생하지 않는다는 원심과 대법원의 판단은 공인인증서 발급절차를 둘러싼 현행법상의 문제점을 인식하지 못하고 전자금융거래에서 금융기관의 안전성 확보의무를 지나치게 좁게 해석하였다는 점에서 비판을 면할 수 없을 것이다.

요컨대 본 사안에서는 원고에게 중과실이 있다고 인정할 수는 없고 이용자의 의사에 반하여 공인인증서의 발급이 이루어졌다는 점에서 피고은행이 공인인증서의 위조에 따른 책임(법 제9조 제1항)을 부담한다고 해석하였어야 할 것이다.[41] 그러나 설사 이용자의 중과실을 인정하여 전자금융거래법 제9조에 따른 피고은행의 면책을 이끌어낼 수 있다 하더라도 본 사안에서 피고은행은 전자금융거래법 제21조(안전성의 확보의무) 및 신의칙상 공인인증서의 재발급으로 인하여 이용자에게 손해가 발생하지 않도록 주의를 촉구할 주의의무가 있었다고 보아야 하기 때문에, 피고은행은 공인인증서의 재발급 사실을 원고에게 알리지 않은데 대해 과실로 인한 불법행위방조책임(민법 제760조 제3항)을 부담한다고 해석하였어야 할 것이다.

41) 그후 개정된 현행 전자금융거래법하에서는 "정보통신망에 침입하여 부정한 방법으로 획득한 접근매체의 이용으로 발생한 사고"(법 제9조 제1항 제3호)에 따른 책임을 금융기관이 부담하는 것으로 해석하게 될 것이다.

VI. 결론에 갈음하여 – 전자금융거래에서 정보보안과 금융소비자보호를 위하여

법리적으로는 본 판결을 위와 같이 이해하고 평가할 수 있지만, 이하에서는 전자금융거래에서 정보보안 및 이용자(금융소비자) 보호라는 보다 거시적인 관점에서 본 판결의 문제점 및 향후의 과제를 간단히 제시하기로 한다.

1. 본 판결은 이른바 개인정보 및 금융거래정보의 유출이 사회문제화 되고 있는 상황에서 보이스피싱 등의 전자금융사기에 의해 발생한 금융소비자의 손해에 대해 그 배상책임을 금융기관에게 물을 것인가가 문제된 최초의 대법원 판결이라는 점에서 대단히 중요한 의미를 갖는다. 단순히 보이스피싱으로 손해를 본 본 사안의 원고에게 배상청구권을 인정할 것인가 말 것인가로 끝나는 것이 아니라 본 판결의 결론에 따라 금융기관의 전자금융거래의 보안수준에 면죄부를 줄 것인가, 아니면 보안수준을 향상시키는 동인을 제공할 것인가가 결정될 수 있었기 때문이다. 그러나 결과적으로 금융소비자보호가 강조되는 상황에서 대법원은 현행 전자금융거래의 보안수준에 심각한 문제가 있다는 점을 인식하지 못하고, 전자금융거래에서 금융기관의 보안수준의 향상이 금융소비자보호에 직결된다는 정책적 배려를 하지 못한 채 피고은행 측 주장을 받아들여 금융거래정보의 노출이 곧 금융사고로 이어질 수 있기 때문에 원고에게 중과실을 인정할 수 있다는 형식적인 법논리에 입각한 판단을 하고 말았다. 그러나 이로써 전자금융거래에 대한 금융소비자들의 불신은 한층 강해질 것이라는 점에서, 본 판결은 금융기관 측에도 결코 유리한 것이라고는 할 수 없다고 생각한다. 본 판결에서 대법원이 금융기관의 책임을 인정하였다면 전자금융거래에서 정보보안이 심각하게 문제되고 있는 상황에서 금융기관이 보안수준을 자발적으로 향상시킬 수 있는 절호의 기회였다는 점에서 본 판결의 결론에는 더욱 아쉬움이 남는 것이다.

따라서 당분간은 금융감독당국에 의한 타율적이고 유동적인[42] 정책에 따라 전자금융거래의 보안수준이 좌우될 수밖에 없는 상황이라고 할 것이다.

2. 전자금융거래법에서 접근매체의 위조나 변조로 발생한 사고에 대하여 원칙적으로 금융기관이 그 책임을 부담하기로 하면서 다만 이용자의 중과실이 있는 경우에만 예외적으로 금융기관이 면책되도록 한 것은 이용자(금융소비자) 보호를 실현하고자 한 입법자의 의사를 반영한 것이다. 그러나 본 판결에서는 제3자의 교묘한 기망행위가 개입되었음에도 불구하고 이를 면밀히 검토하지 않은 채 이용자의 직업과 금융거래 경험이라는 주관적인 요소 및 전화금융사기에 대한 사회적 경각심이 높아진 상태였다는 지극히 추상적인 이유로 이용자의 중과실을 인정해 버렸기 때문에, 본 판결에 따라 향후에 이용자에게는 '과실'과 유사한 (또는 그 이상의) 주의의무가 요구된 것과 마찬가지의 결과가 되었다고 할 것이다. 더욱이 본 사안에서는 제3자가 공인인증서의 발급절차가 대단히 취약한 상황임을 이용하여 공인인증서를 재발급 받았음에도 불구하고 본 판결은 이에 관하여 아무런 고려를 하고 있지 않다. 그렇다면 결과적으로 위와 같은 입법자의 의사 내지 전자금융거래의 안전성을 최고의 이념으로 삼는 전자금융거래법의 입법취지가 무색하게 되는 것은 아닌지 우려된다. 이와 같은 점을 고려한다면 본 판결에서 대법원이 제시한 이용자의 중과실 판단기준에는 향후에 "금융기관의 전반적인 정보보안의 수준"이 추가되는 것이 타당하다고 생각한다. 이 기준이 추가된다면 금융기관의 정보보안이 취약할 경우에는 이용자의 중과실도 보다 신중하게 판단하도록 제어하는 역할을 하게 될 것이기 때문이다.

3. 본 판결을 계기로 입법론적으로 심각하게 고민하여야 할 과제가 등장하였다. 공인인증서의 발급절차를 규정하는 전자서명법 시행규칙(제13조의2 제4항)은 전술

42) 중앙일보, 2014.4.17. 기사, "26개 금융사, 5년간 IT검사 한 번도 안 받았다"; 디지털타임스, 2014.4.16. 기사, "당장 암호화 한다더니… '뻔뻔한 금융권'"; MK뉴스 2014.2.10. "[ISSUE INSIDE] 오락가락 금융당국…밀어붙이다 여론 나쁘면 후퇴 되풀이" 등 참조 .

한 바와 같이 접근매체로서의 공인인증서의 발급절차상의 편의성을 고려한 입법이지만 현재는 전자금융거래의 안전성을 해하는 결정적인 근거규정이 되고 있다는 점이다. 따라서 동 규정은 하루속히 삭제하거나 개선책을 마련하여야 할 것이다.[43] 물론 이를 통하여 전자금융거래의 편의성은 다소 감소할 수 있고 금융기관의 업무부담이 늘어날 가능성도 존재한다. 그러나 전자금융거래에서 접근매체, 특히 공인인증서의 중요성을 감안해볼 때 그 발급은 대면을 통하여 철저하게 이루어져야 거래 전체의 안전성이 확보될 수 있다는 점은 아무리 강조해도 지나치지 않는다. 접근매체의 발급절차상의 안전성이 확보된다면 이용자에게 그 사용상의 책임을 묻기도 훨씬 수월해질 것이다. 반면에 현재와 같이 정보보안이 취약한 상황에서 금융기관이 자신의 면책(무과실)을 주장하고 이용자에게 그 책임(중과실)을 묻는 것은 너무나 무책임한 태도라고 하지 않을 수 없다.

한편 전자금융거래에서 공인인증서와 같이 공인된 접근매체를 사용하도록 정책적으로 강제하는 경우는 비교법적으로 흔하지 않다. 그럼에도 불구하고 전자금융사기에 의한 피해가 급증하고 있는바 이러한 정책 내지 제도를 철폐하여 인증시장의 경쟁을 유도하고 정보보안의 수준을 향상시키자는 주장이 제기되는 것도 무리는 아니다.[44] 그러나 필자는 공인인증서 발급절차상의 안전성이 확보된다면 공인인증서의 존폐여부를 둘러싼 논의에도 상당부분 영향을 미칠 것이라 생각한다. 공인인증서를 통한 전자금융거래라는 현 제도의 틀을 무작정 철폐하기 보다는 발급절차를 보다 엄격하게 함으로써 정보보안 상의 많은 문제점이 해소될 수 있다고 생각하기 때문이다.

---

43) 이와 같은 문제의식에 따라 행정안전부(2012.6.25. 당시)로부터 전자서명법 시행규칙 개정안이 입법예고되었다(행정안전부 2012.6.26. 보도자료). 이 개정안에서는 본인확인 절차로서 단말지정, 전화승인, OTP+SMS 등의 '추가인증수단' 중에서 이용자가 하나를 선택하도록 하고 있다. 그러나 본인확인 절차가 강화되었다는 점에서는 개선이라고 할 수 있으나 "정보통신망상의 본인확인"이라는 점에는 변함이 없기 때문에 보다 확실하게는 대면확인에 의하도록 하는 것이 正道라고 생각한다. 강화된 공인인증서 재발급 절차는 2014년 1월부터 본격 적용된다는 것이 위 보도자료의 설명이나, 아직 전자서명법 시행규칙에는 반영되지 않고 있다.

44) 예컨대, 최재천 의원 대표발의 "전자서명법 전부개정법률안"(2013.5.28. 제안)은 현행 공인인증제도의 철폐를 목적으로 한 것이다.

〈참고문헌〉

1. 단행본

손진화, 전자금융거래법[제2판], 법문사(2008)
정경영, 전자금융거래와 법, 박영사(2007)
高見澤昭治・齋藤雅弘・野間啓 編著『預金者保護法ハンドブック』(日本評論社、2006)

2. 논문

강성복・윤종민, "전기통신금융사기 법제에 관한 분석적 고찰", 과학기술과 법 제3권 제2호(2012.12)
김병태, "예금통장(대포통장)은 전자금융거래법상의 접근매체인가?-대법원 2010.05.27. 선고, 2010도2940 판결-", 선진상사법률연구 통권 제54호(2011.4)
박지현, "전자금융거래시 공인인증서 의무사용 규제완화 관련 주요이슈 및 현황", 지급결제와 정보기술(2010.7)
서희석, "훔친 통장과 인장을 이용한 예금인출의 유효성-대법원 2007.10.25. 선고 2006다44791 판결에 대한 비판적 검토-", 소비자문제연구 제35호(2009.4)
이정현, "2006년 시행 전자서명법의 개정내용과 향후 과제", 정보보호 정책동향(한국정보보호진흥원)(2006년)
徐熙錫「電子金融取引の民事法理(1)(2)(3・完)-韓国電子金融取引法の考察-」一橋法学第5巻3号・第6巻第1号・第6巻第3号(2006.11・2007.3・11)
松本恒雄「預金者保護に向けた法整備と残された課題」自由と正義57巻3号(2006.3)

투 고 일 : 2014년 4월 23일
심 사 일 : 2014년 5월 9일
수 정 일 : 2014년 5월 16일
게재확정일 : 2014년 5월 23일

주제어 : 전자금융거래법, 접근매체, 공인인증서, 시스템거래, 보이스피싱, 금융소비자, 정보보안, 전자금융거래의 안전성

〈Abstract〉

Judgment Criteria for "User's Gross Negligence" under Electronic Financial Transaction Act

by Heesok Seo

The present decision has great significance as the first Supreme Court ruling over an issue regarding the liability of a financial institution for losses suffered by the user of electronic financial transaction due to electronic financial fraud methods like voice phishing. In the ruling, the Supreme Court presented judgment criteria that whether or not there is "intention or gross negligence of the user", a condition for liability exemption of financial institutions under the Electronic Financial Transaction Act, shall be "judged by consideration on details of the financial accident like forgery of the means of access, the substance of the method like forgery and perception of the general public on the method, occupation and experience of the user of the financial transaction, and the totality of circumstances." Based on this judgment criteria, the court ruled in the present case that the user was grossly negligent, and the financial institution was thus exonerated from liability. It can be said that auser's duty of care toward future electronic financial fraud will be more "strictly" required after this decision. However, the present decision is difficult to support in that: (1) the decision, which equated exposure of financial transaction information with that of the access means, went beyond the scope of textual interpretation of the Act; (2) it hardly conducted assessment on the fraudulent act by a third part; and furthermore, (3) it gave the security level of the financial institution no consideration. It would be more reasonable if the "overall security level of the financial institution" was added to the judgment criteria for user's gross negligence presented by the Supreme Court in the future. It is because the addition of this criterion would play a controlling

role in influencing courts to be more cautious in deciding a user's gross negligence, particularly in cases where the information security systems were vulnerable.

Key Words : Electronic Financial Transaction Act, Means of Access, Authorized Certificate, System Transaction, Voice Phishing, Financial Consumer, Information Security, Electronic Financial Transaction Safety