전자금융거래 사고에 대한 손해배상책임

이 지 언 (자본시장연구실, 선임연구위원, 3705-6352)

〈요 약〉

□ 전자금융거래법은 전자금융거래 사고 피해 구제를 위해 일정한 경우 정책적 차원에서 금융회사에게 무과실 손해배상책임을 부과하고 있으나, 제도의 취지에도 불구하고 피해자가 배상을 받는 데는 제도적 장애요인이 많음.

□ 현행법에 따르면 피해자가 사고 관련 전자금융거래 정보를 취득·분석해서 사고 원인을 기술적으로 입증해야 하는데, 이는 기술 전문지식이 없는 피해자에게는 매우 큰 부담임.

□ 또한 현행법이 무과실 손해배상책임이 인정되는 사고 및 범죄 유형을 제한적으로 열거하고 있기 때문에 날로 지능화·다양화하는 전자금융사기 피해에 관한 법률 분쟁에서 소비자가 구조적으로 불리함.

□ 따라서 향후 전자금융거래법을 개정할 때 금융회사의 무과실책임 요건을 보다 포괄적으로 규정할 필요가 있는데, 우선 사고 원인에 대한 입증책임을 금융회사에게 부담시키는 방안을 고려해야 함.

□ 또한 사고·범죄 유형을 복잡한 기술적 사실에 제한하지 말고 포괄적으로 정의함으로써 피싱·스미싱 등에 의한 피해도 구제받도록 해야 함.

현행 전자금융거래법(이하 법) 및 그 시행령(이하 시행령)은 이용자의 전자금융거래 사고 피해 구제를 위해 일정한 경우 금융회사에게 무과실 손해배상책임을 부과하고 있다. 무과실책임 제도의 취지는 금융회사가 운영 · 관리하는 고도의 기술적 영역인 전자금융거래시스템에서 사고가 발생하였다면 정책적 관점에서 비록 금융회사는 과실이 없더라도 배상해야 한다는 것이다. 그러나 사고가 발생하였을 때 피해자가 실제로 배상을 받기가 매우 어려워 제도의 취지가 퇴색되고 있다는 지적이 많다. 이에 따라 본고에서는 관련 제도를 살펴보고, 개선방향을 제시하고자 한다.

전자금융거래법상 무과실책임의 개요

현행법에 따르면 전자금융거래 사고가 발생했을 때 다음 요건들이 모두 충족되면 금융회사 또는 전자금융업자(이하 금융회사)는 무과실 손해배상책임을 진다(법 9조, 10조). ① 고객이 개인 또는 소기업(중소기업기본법)이어야 한다. 따라서 고객이 중 · 대기업이면, 금융회사는 과실이 있는 경우에만 손해배상책임이 있고, 무과실책임은 지지 않는다. ② 금융회사가 관리하는 기술적 영역에서 발생한 사고여야 한다. 법이 인정하는 기술적 사고들은 접근매체의 위 · 변조, 거래 체결 · 지시의 전송 · 처리과정에서의 사고, 정보통신망 침입(hacking)이다. 단, 사고가 이러한 영역에서 발생하였음을 피해자가 입증해야 한다. 사고가 금융회사 통제 밖에서 발생한 경우(접근매체 도난 · 분실)에는 통지 이후의 손해에 대해서만 금융회사가 배상책임을 부담한다. ③ 고객이 무과실이거나 과실이 있더라도 경과실이어야 한다.[1] 고객에게 고의 또는 중과실(접근매체 대여, 제공, 누설, 노출, 방치, 추가보안 조치 거부 ; 시행령 8조)이 있으면 금융회사는 무과실책임을 면하게 된다. 단, 금융회사가 고객의 중과실을 입증해야 한다.

위에서 언급된 접근매체(means of access to the account ; 법 2조 10호)란 전자금융거래 지시의 주체와 내용의 진실성을 확보 · 확인할 수 있는 수단이나 정보로서 스마트카드, 인증서, 전자서명생

1) 과실이란 주의의무 위반을 의미하며, 무과실이란 합리적으로 요구되는 충분한 주의의무를 다한 경우를 말한다. 고의(악의, 사기)가 있는 자는 어떤 경우에도 책임을 진다.

성정보, 생체정보 등을 말한다.[2] 단, 계좌번호, 계좌비밀번호, 이체비밀번호, 보안카드 · OTP생성기 비밀번호(일회용 비밀번호)는 법상 접근매체로 열거되어 있지 않다. 접근매체는 사고 원인과 관련하여 쟁점이 되는 중요한 개념이다.

전자금융거래 사고 사례와 법률적 쟁점 분석

아래에서는 전형적인 피해 사례를 가지고 법률적 쟁점을 살펴보기로 한다.

① 해커가 피해자의 PC나 USB 저장장치에 침입하여 공인인증서 파일을 무단 복제한 경우, 이를 접근매체의 위조(금융회사의 무과실 손해배상책임 발생)로 볼 것인지 논란이 있다. 대체로 학설과 판례는 피해자의 의사에 반하여 권한이 없는 자가 파일을 복제한 것은 위조로 본다.

② 접근매체(공인인증서 등)를 도난 · 분실한 경우, 이를 무단 복제와 마찬가지로 접근매체의 위조로 볼 것인지 논란이 있다. 접근매체의 도난 · 분실이란 사실상의 지배(점유)를 잃는 상태로서 PC나 USB 저장장치 자체를 도난당한 것을 말한다. 앞선 ①의 경우는 소프트웨어의 도난인데 비해 ②의 경우는 하드웨어의 도난이라는 점에서 차이가 있다. 이 경우는 금융회사가 관리할 수 없는 영역에서의 사고이기 때문에 사고 통지 이후의 손해에 대해서만 금융회사가 배상책임을 진다(법 10조). 만약 피해자가 통지 이전의 손해에 대해서도 배상받고자 한다면 두 가지 중 하나를 주장해야 한다. 첫째, 하드웨어 도난 · 분실로 인해 접근매체의 위조가 행해졌다고 주장하는 것이다. 앞선 ①의 경우처럼 인증서 파일을 무단 복제해서 사용하면 위조이므로, 훔친 파일을 복제하지 않고 그대로 사용하는 것도 위조로 보아야 한다(양자는 파일을 훔쳤다는 점에서 같기 때문에 구별할 이유가 없다)는 학설도 있다. 둘째, 피해자가 금융회사에 대해 민사상 과실책임을 묻는 것이다. 이 경우 피해자는 금융회사가 전자금융사기 적발 시스템(fraud detection system : FDS) 운영 등에 있어서 충분한 주의의무를

2) 미국 전자자금이체법은 접근매체를 자신의 계정에 접근 · 접속하는 데 필요한 일체의 수단이라고 포괄적으로 정의한다. 반면 우리나라 전자금융거래법 2조 10호는 접근매체의 종류를 다음과 같이 제한적으로 열거하고 있다. ㉮ 전자식 카드 및 이에 준하는 전자정보와 이들을 사용하는 데 필요한 비밀번호, ㉯ 전자서명생성정보(개인키) 및 인증서와 이들을 사용하는 데 필요한 비밀번호, ㉰ 금융회사에 등록된 이용자 번호(user ID), ㉱ 생체정보.

다하지 않았다는 것을 입증해야 하는데, 현실적으로 매우 어려울 것이다.

③ 보이스 피싱(voice phishing), SMS 피싱(smishing), 파밍(pharming ; 악성코드 감염을 통해 적법을 사칭하는 악성 웹사이트로 접속)을 악용해 취득한 개인정보로 공인인증서(법상 접근매체)를 부정 발급 받은 경우, 이를 접근매체의 위조로 볼 것인지에 대해 여러 피해 사건에서 논란이 있다. 접근매체의 위조로 본다면 금융회사 관리 영역 내에서의 사고이므로 금융회사는 무과실책임을 지게 된다. 공인인증서의 위조를 좁게 해석한다면 해커가 공인인증기관의 고도의 보안시스템을 뚫고 피해자의 인증서를 직접 허위로 작성하는 것이라고 하겠지만, 이는 기술적으로 사실상 불가능하다는 것이 정설이다(세계적으로 거의 유례가 없음). 따라서 피해자 구제 차원에서 인증서 부정 발급을 접근매체의 위조로 보는 것이 타당하며,[3] 이를 인정하는 판례도 있다.

④ 앞에서의 공인인증서 부정 발급에 더해 피해자가 해커에게 계좌비밀번호, 이체비밀번호, 일회용 비밀번호 등을 부주의하게 노출함으로써 발생한 손해에 대해서도 금융회사가 무과실 배상책임을 지느냐가 문제이다. 법 9조와 시행령 8조에 따르면 피해자가 접근매체를 노출하면 중과실에 해당하여 배상을 받을 수 없기 때문에 위의 비밀번호들이 접근매체에 해당하는지가 이슈이다. 대법원 판례는 접근매체에 해당한다고 보는 반면 일부 학설은 접근매체를 제한적으로 열거한 법 2조 10호에 포함되지 않으므로 접근매체가 아니라고 본다. 이처럼 법령 해석이 모호하기 때문에 피해자가 구제를 받기가 현실적으로 매우 어려운 것이다.

제도적 장애요인과 개선방향

위의 여러 사례들을 종합해 볼 때 피해자 구제가 어려운 가장 큰 이유는 사고 원인을 피해자가 기술적으로 입증해야 한다는 점이다. 그러나 정보통신기술의 전문성과 비대칭성으로 인해 이는 현실

3) 인증서가 부정한 방법으로 발급되었더라도 공인인증기관이 직접 발행한 것은 사실이므로 인증서 자체가 위조된 것은 아니다. 또한 금융회사가 알기 어려운 부정 발급을 위조로 인정해 무과실책임을 부과하는 것은 금융회사에게 지나치게 불리하다는 견해도 있다. 그러나 또 다른 견해는 인증서를 발급받기 위해서는 범인이 자신의 PC · USB 등에 개인키 파일(정당한 소유자에게 귀속되어야 함)을 직접 생성해야 하므로 위조라고 본다.

적으로 매우 어렵다. 예컨대 피해자가 공인인증서를 무단 복제당한 경우 '접근매체의 위조'에 해당하므로 배상받을 수 있지만 기술 전문지식이 없는 피해자가 관련 전자금융거래 정보를 취득 · 분석해서 원인과 손해의 인과관계까지 밝히는 것은 거의 불가능할 것이다. 따라서 향후 전자금융거래법을 개정할 때 전자금융거래 사고의 원인에 대한 입증책임을 금융회사에게 부담시키는 방안을 고려해야 한다. 즉 해당 사고가 금융회사 통제 밖에서 일어난 사고라는 것을 금융회사가 입증토록 하는 것이다.

피해자 구제가 어려운 또 다른 이유는 현행법이 사고 또는 범죄의 유형을 제한적으로 열거하고 있다. 접근매체의 위 · 변조를 예로 들면, 접근매체의 유형을 제한적으로 열거하고, 범죄의 유형도 위 · 변조에 한정하고 있다. 이에 따라 위 · 변조인지에 관한 논란이 빈발하고 있는 실정이다. 그러나 정보통신기술의 발달과 함께 접근매체도 다양화할 뿐만 아니라 전자금융사기도 지능화 · 정교화하고 있어 새로운 매체와 사기 수법에 관한 법률 분쟁에서는 소비자가 구조적으로 불리할 것이다.

따라서 금융회사 무과실책임 요건을 복잡한 기술적 사실로 제한(예컨대 접근매체의 유형을 특정하거나 범죄 유형을 위 · 변조 등에 한정)하지 말고 포괄적으로 정의함으로써 피싱 · 스미싱 등에 의한 피해도 구제받도록 해야 한다. 접근매체를 이용자의 계정(account)에 접근 · 접속하는 데 필요한 일체의 수단이나 도구로 정의하고, 이를 부정하게(기망 등을 통해 정당한 권리자의 의사에 반하여) 사용하면 금융회사의 무과실책임이 성립하도록 해야 한다.

다만 법 개정 과정에서 고려해야 할 점은 우리나라에서는 개인정보가 엄격히 보호되고 있을 뿐만 아니라 금융회사에게는 강력한 조사권이 없기 때문에 금융회사의 무과실책임을 과도하게 높이면 이용자의 사기 공모 등이 빈발할 우려도 있다는 것이다. 따라서 금융회사가 사고의심 거래(또는 계좌)를 일정 시간 지연(동결)하거나 조사하도록 하는 방안을 강구해야 한다. KIF