



제433회국회(임시회)
제1차 정무위원회

전자금융거래법 일부개정법률안

검 토 보 고

〈 계열회사 침해사고 통지 의무 신설 〉

■ 김현정의원 대표발의(의안번호 제2215866호)

2026. 3.

정 무 위 원 회
수석전문위원 정 명 호

목 차

I . 제안경위	1
II . 제안이유 및 주요내용	1
III . 검토의견: 계열회사 침해사고 통지 의무 신설	3

I. 제안경위

1. 제 안 자 : 김현정의원 등 12인
2. 제 안 일 : 2026. 1. 6.
3. 회 부 일 : 2026. 1. 7.

II. 제안이유 및 주요내용

현행법은 금융회사 및 전자금융업자로 하여금 침해사고의 발생 시 금융위원회에 즉시 통지할 의무를 부여하고 있는데, 최근 특정 온라인 쇼핑몰 업체에서 대규모 개인정보 유출사태가 발생함에 따라 침해사고의 통지의무를 보다 확대하는 방향으로 개선할 필요성이 제기됨.

최근 발생한 침해사고의 경우 온라인쇼핑몰을 운영하는 전자상거래 사업자와 전자지급결제대행회사가 계열회사 관계로, 하나의 이용자번호 등의 접근매체로 접속하여 별도 결제 정보 입력 없이 간편결제할 수 있도록 하는 서비스를 제공하고 있는데, 온라인쇼핑몰을 통한 접근매체 등 정보 유출에 따라 전자지급결제대행회사의 결제정보까지 유출될 우려가 제기됨. 그러나 전자상거래 사업자는 현행법상 금융회사 등에 해당되지 아니하여 사고가 발생하여도 금융위원회에 대한 통지

의무 등을 포함한 현행법상 규제의 적용 대상이 되지 않음.

이에 침해사고의 통지 의무 대상에 동일 접근매체의 사용 등으로 인하여 계열회사에서 발생한 사고의 영향을 받을 가능성이 있는 경우도 포함하도록 함으로써 연이어 발생하는 개인정보 유출 등의 침해사고를 적극적으로 방지하고자 함(안 제21조의5제2항 및 제3항 등).

Ⅲ. 검토의견: 계열회사 침해사고 통지 의무 신설

- 개정안은 금융회사 및 전자금융업자가 자신의 계열회사에서 침해사고가 발생하여 접근매체가 유출될 우려가 있는 등 대통령령으로 정하는 경우에는 금융위원회에 지체 없이 계열회사 침해사고의 발생 사실, 유출 정보, 접근매체 또는 금융정보와의 유사성 등을 알리도록 하고, 침해사고의 원인과 피해확산 방지 조치를 하도록 하도록 하는 내용임.

현행	개정안
제21조의5(침해사고의 통지 등) ① (생략) <u><신설></u>	제21조의5(침해사고의 통지 등) ① (현행과 같음) ② <u>금융회사 및 전자금융업자는 계열회사(「독점규제 및 공정거래에 관한 법률」 제2조제12호에 따른 계열회사를 말한다. 이하 같다)에서 이용되는 정보시스템 또는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호에 따른 정보통신망이 교란·마비되는 등의 사고(이하 “계열회사침해사고”라 한다)가 발생한 경우로서 접근매체의 유사성으로 인하여 접근매체가 유출될 우려가 있는 등 대통령령으로 정하는 경우에는 금융위원회에</u>

현행	개정안
② 금융회사 및 전자금융업자는 <u>침해사고</u>가 발생하면 그 원인을 분석하고 피해의 확산을 방지하기 위하여 필요한 조치를 하여야 한다.	<u>지체 없이 계열회사침해사고의 발생 사실, 이로 인하여 유출된 정보, 그리고 접근매체 또는 금융 정보와의 유사성 등을 알려야 한다. 이 경우 구체적인 적용대상 및 내용 등 통지에 필요한 사항은 대통령령으로 정한다.</u>
제43조(허가와 등록의 취소 등) ① (생략) ② 금융위원회는 금융회사 또는 전자금융업자가 다음 각 호의 어느 하나에 해당하는 때에는 6월의 범위 안에서 기간을 정하여 관련 업무의 전부 또는 일부의 정지를 명할 수 있다. 1. 제6조제1항·제2항, 제16조제1항부터 제4항까지, 제19조제1항, 제21조제1항·제2항, <u>제21조의5 제2항</u>, 제25조의2제1항, 제35조, 제35조의2제2항·제3항, 제36조	③ ----- <u>침해사고(계열회사침해사고를 포함한다)</u>----- ----- ----- --. 제43조(허가와 등록의 취소 등) ① (현행과 같음) ② ----- ----- ----- ----- ----- -----. 1. ----- ----- -----<u>제21조의5 제3항</u>----- -----

현행	개정안
또는 제38조제3항·제4항의 규정을 위반한 때	----- -----
2. ~ 4. (생략)	2. ~ 4. (현행과 같음)
③·④ (생략)	③·④ (현행과 같음)
제51조(과태료) ①·② (생략)	제51조(과태료) ①·② (현행과 같음)
③ 다음 각 호의 어느 하나에 해당하는 자(제1호, 제6호부터 제8호까지 및 제10호의 경우에는 제28조제4항에 따라 해당 규정을 준용하는 선불전자지급수단을 발행하는 자를 포함한다)에게는 1천만원 이하의 과태료를 부과한다.	③ ----- ----- ----- ----- ----- -----.
1. ~ 6. (생략)	1. ~ 6. (현행과 같음)
<u><신설></u>	<u>6의2. 제21조의5제2항을 위반하여</u> <u>계열회사침해사고를 알리지 아니한 자</u>
7. ~ 12. (생략)	7. ~ 12. (현행과 같음)
④ (생략)	④ (현행과 같음)

□ 현행법 제21조의5¹⁾에 따르면, 금융회사 및 전자금융업자는 전자적 침

1) 「전자금융거래법」

제21조의5(침해사고의 통지 등) ① 금융회사 및 전자금융업자는 전자적 침해행위로 인하여 전자금융기반시설이 교란·마비되는 등의 사고(이하 “침해사고”라 한다)가 발생한 때에는 금융위원회에 지체 없이 이를 알려야 한다.

② 금융회사 및 전자금융업자는 침해사고가 발생하면 그 원인을 분석하고 피해의 확산을 방지하기 위하여 필요한 조치를 하여야 한다.

해행위로 인하여 전자금융기반시설이 교란·마비되는 등의 침해사고가 발생한 경우 이를 지체 없이 금융위원회에 통지하도록 하고 있음. 이를 위반하여 침해사고를 알리지 않은 경우 1천만원 이하의 과태료가 부과됨.

□ 그런데, 전자상거래 사업자와 전자금융업자 등이 서로 계열회사 관계에 있으면서 이용자번호 등 접근매체를 공유하는 상황에서, 전자상거래 사업자의 개인정보 유출 사고가 발생한 경우 계열회사인 전자금융업자 등의 정보유출 사고로 이어질 위험이 있음에도 불구하고 이런 경우에는 전자금융업자 등이 금융위원회에 사고 사실 등을 통지할 의무가 없어, 효과적인 대응에 한계가 있다는 문제제기가 있음.

□ 이에 개정안은 계열회사의 침해사고가 발생한 경우로서 접근매체²⁾의 유사성으로 인하여 접근매체가 유출될 우려가 있는 등의 경우에는 금융회사·전자금융업자가 계열회사의 침해사고 사실, 유출정보 등을 금융위원회에 지체 없이 알리도록 하고, 미통지 시 과태료를 부과하도록 하며, 계열회사의 침해사고 발생에 대한 원인 분석 및 확산 방지 조치를 하도록 함으로써,

2) 「전자금융거래법」

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

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」 제2조제3호에 따른 전자서명생성정보 및 같은 조 제6호에 따른 인증서

다. 금융회사 또는 전자금융업자에 등록된 이용자번호

라. 이용자의 생체정보

마. 가목 또는 나목의 수단이나 정보를 사용하는데 필요한 비밀번호

침해사고의 피해 확산을 방지하고 효과적인 대응을 하려는 취지임.

□ 금융회사·전자금융업자와 계열회사가 서로 이용자 번호 등을 공유하는 구조인 경우(이른바 One-ID 시스템), 계열회사의 정보유출에 따른 피해의 위험 또한 서로에게 미칠 수 있을 수 있으므로 그 책임 또한 공유함으로써 효과적으로 피해를 예방하고 금융소비자를 두텁게 보호하려는 취지는 긍정적인.

□ 다만, 어떤 회사에 침해사고가 발생한 경우 그 사실을 계열회사 관계에 있는 금융회사 등에게 알려야 할 의무가 있지는 않으므로, 실제로 금융회사 등이 금융위원회에 통지를 하기 위해서는 계열회사의 임의적인 협조를 받아야 함. 이러한 현실적인 제약이 있는 상황에서 통지의무를 부과하고 위반시 과태료까지 부과하는 것은 과도한 측면도 있음.

또한, 개정안은 계열회사 침해사고에 대해 금융회사 등이 계열회사 침해사고의 원인 분석과 피해 확산 방지조치를 하도록 규정하고 있는데, 금융회사 등이 계열회사에 대한 실질적인 조사권한이나 조치권한을 가지고 있다고 보기 어렵기 때문에 이러한 의무를 이행하는 것은 사실상 어려운 측면이 있음.

○ 참고로, 금융감독원은 현행법 제39조³⁾에 근거하여 금융회사·전자금

3) 「전자금융거래법」

제39조(감독 및 검사) ①금융감독원(「금융위원회의 설치 등에 관한 법률」 제24조제1항의 규정에 따른 “금융감독원”을 말한다. 이하 같다)은 금융위원회의 지시를 받아 금융회사 및 전자금융업자에 대하여 이 법 또는 이 법에 의한 명령의 준수여부를 감독한다.

유통거래업자에 대한 일반적인 감독 및 검사 권한을 갖고 있고, 금융회사·전자금융업자의 계열회사에서 침해사고가 발생한 사실을 인지할 경우 조사 등을 할 수 있음.

다만, 해당 침해사고의 발생사실에 대해 신속하게 인지하지 못하는 경우가 발생할 수 있으므로, 개인정보보호위원회, 과학기술정보통신부 등 유관부서와 정보 공유 등 효과적인 공동 대응 방안을 강구해 나갈 필요가 있어 보임.

□ 개정안에 대하여, 금융위원회는 개정안의 취지에는 공감하나, 실무적 제약 및 실효성 등을 감안할 때 신중한 검토가 필요하다는 입장이고, 한국온라인쇼핑협회에서는 별개 법인인 계열회사의 침해사고에 대한 통지 및 원인분석 등의 의무 부과는 책임주의 원칙에 반하는 등 신중한 검토가 필요하다는 의견을 제시함.

②금융감독원장은 제1항의 규정에 따른 감독을 위하여 필요한 때에는 금융회사 또는 전자금융업자로 하여금 그 업무 및 재무상태에 관한 보고를 하게 할 수 있다.

③금융감독원장은 금융회사 및 전자금융업자의 전자금융업무와 그와 관련된 재무상태를 검사하고, 검사를 위하여 필요하다고 인정하는 때에는 금융회사 및 전자금융업자에 대하여 업무와 재무상태에 관한 자료의 제출 또는 관계인의 출석을 요구할 수 있다.

④제3항의 규정에 따라 검사를 하는 자는 그 권한을 표시하는 증표를 지니고 이를 관계인에게 내보여야 한다.

⑤금융감독원장은 제3항의 규정에 따라 검사를 한 때에는 그 결과를 금융위원회가 정하는 바에 따라 금융위원회에 보고하여야 한다.

⑥금융위원회는 금융회사 또는 전자금융업자가 이 법 또는 이 법에 따른 명령을 위반하여 금융회사 또는 전자금융업자의 건전한 운영을 해할 우려가 있다고 인정하는 때에는 금융감독원장의 건의에 따라 다음 각 호의 어느 하나에 해당하는 조치를 하거나 금융감독원장으로 하여금 제1호부터 제3호까지에 해당하는 조치를 하게 할 수 있다.

1. 위반행위에 대한 시정명령
2. 금융회사 또는 전자금융업자에 대한 주의 또는 경고
3. 임원과 직원에 대한 주의, 경고 또는 문책의 요구
4. 임원(「금융회사의 지배구조에 관한 법률」 제2조제5호에 따른 업무집행책임자는 제외한다. 이하 제39조의2에서 같다)의 해임권고 또는 직무정지

문 의 처

02)6788-5104
