



제 429국회 (정기회)
제 10차 정무위원회

전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법 일부개정법률안

검 토 보 고

〈전기통신금융사기 관련 정보공유분석기관의 설치 등〉
■ 강준현의원 대표발의(의안번호 제2214027호)

2025. 11.

정 무 위 원 회

수석전문위원 정명호

목 차

I. 제안경위	1
II. 제안이유 및 주요내용	1
III. 검토의견	3
1. 개정안의 주요 내용	3
2. 개정안의 발의 배경 및 필요성	4
3. 주요 내용별 검토	8
가. 사기관련의심제좌 정의 신설	8
나. 전기통신금융사기 관련 정보공유 체계 수립	13
다. 전기통신금융사기 관련 정보의 공유·처리 관련 안전조치 ...	24
라. 개별법상 정보보호 규정 관련 특례	26
[참고1] 통신사기피해환급법 주요내용	30
[참고2] 보이스피싱 AI 플랫폼(ASAP) 개요	32
[참고3] 금융보안원 개요	33

I. 제안경위

1. 제 안 자 : 강준현의원 등 13인
2. 제 안 일 : 2025. 11. 7.
3. 회 부 일 : 2025. 11. 10.

II. 제안이유 및 주요내용

최근 보이스피싱 등 전기통신금융사기가 급속히 진화·지능화됨에 따라 금융회사의 자체 이상거래탐지시스템(FDS)만으로는 신속한 대응에 한계가 있음. 또, 각 금융회사가 개별적으로 보유한 의심계좌·거래정보만으로는 범죄 패턴을 종합적으로 파악하기 어렵고, 수사기관 및 전기통신사업자와의 정보공유 체계가 미비하여 범죄 확산 방지에 제약이 있음. 특히, 피해계좌나 사기이용계좌 관련 정보가 탐지되더라도 이를 즉시 다른 금융회사나 통신사업자에게 전달할 수 있는 단일한 공유채널이 없어 신속한 대응이 곤란하며, 금융회사 간 AI 기반 탐지 역량의 격차로 인해 신종 수법에 대한 공동 대응도 어려운 상황임.

이에 전기통신금융사기 발생 이전 단계에서 금융회사가 선제적으로 범죄 의심계좌 등을 탐지하고 지급정지 등 조치를 취할 수 있도록, 금융·수사·통신 분야의 의심정보를 공유·분석할 수 있는 정보공유분석기관을 금융위원회가 지정·운영하도록 하고자 함.

아울러 정보공유분석기관에 제공되는 정보 및 제공 주체의 범위를 구체적으로 규정하는 한편, 공유·분석되는 정보의 보호 및 보안 등을 위하여 정보공유분석기관의 기술적·물리적·관리적 대책 수립 의무를 명시하고자 함. 또, 정보공유분석기관 및 정보제공기관 등이 처리한 정보의 목적 외 사용 금지 및 정보보유 기간 제한 등 안전한 활용 기준을 마련하여 금융사기 예방체계를 실질적으로 강화하고 국민의 재산 피해를 최소화하고자 함(안 제2조제8호·제13조의4 신설).

Ⅲ. 검토의견

1. 개정안의 주요 내용

구 분	주요 내용
사기관련의심계좌 정의 신설 (§2-8, 신설)	• 사기관련의심계좌의 정의 신설 ※ 전기통신금융사기에 관련된 것으로 의심되는 계좌로서 사기범의 계좌와 피해자의 계좌 모두 포괄
정보공유분석기관의 지정 등 (§13의4①)	• 정보공유분석기관*의 지정 * 전기통신금융사기에 관한 정보를 제공받아 분석하여 공유하는 기관 • 사기정보제공기관의 범위 규정 ※ 금융회사, 전기통신사업자, 수사기관, 그 밖에 대통령령으로 정하는 자 • 정보공유분석기관에 대한 사기정보제공기관의 사기 관련 정보 제공 근거 마련
사기정보제공기관의 사기 관련 필수정보 제공 의무화 (§13의4②)	• 정보공유분석기관의 요청 시 사기정보제공기관의 사기 관련 필수정보 제공 의무화
정보공유분석기관의 사기 관련 정보 제공 등 (§13의4③)	• 사기정보이용기관의 범위 규정 ※ 금융회사, 그 밖에 대통령령으로 정하는 자 • 사기정보이용기관에 대한 정보공유분석기관의 사기 관련 정보 제공 근거 마련
제공받은 정보의 처리 (§13의4④)	• 제공받은 정보(주민등록번호 포함)에 대한 사기정보이용기관 및 정보공유분석기관의 처리 근거 마련
안전성 확보 조치 등 (§13의4⑤, ⑦)	• 정보공유분석기관의 안전성 확보 조치 의무화 • 사기정보제공기관, 사기정보이용기관 및 정보공유분석기관의 사기 관련 정보 처리 시 준수사항 규정
정보 제공의 특례 (§13의4⑥)	• 금융거래정보 및 개인신용정보의 제공 관련 특례 규정 ※ 「금융실명거래 및 비밀보장에 관한 법률」 및 「신용정보의 이용 및 보호에 관한 법률」 관련 특례
세부사항의 시행령 위임 (§13의4⑧)	• 사기 관련 정보의 제공 및 처리, 정보공유분석기관의 지정 절차 등에 필요한 사항을 대통령령에 위임

2. 개정안의 발의 배경 및 필요성

□ 최근 고도화된 시나리오, AI·딥페이크 기술 등 IT기술의 비약적 발전 등으로 보이스피싱 범죄수법이 첨단화·다양화되며 금융소비자 피해 규모도 빠르게 확대¹⁾되는 양상을 보이고 있음.

○ 보이스피싱 범죄조직들이 해외에 거점을 두고 특정 소비자를 타겟팅하여 대규모의 자금을 편취하고 신속히 도주하는 사례가 발생하고 있고²⁾, 가상계좌, 간편송금 등을 이용하여 단기간에 여러 계좌로 이체를 반복하는 방식으로 자금추적을 회피하는 경우가 다수 발생하고 있는바, 관련 기관 간의 체계적이고 신속한 정보 공유를 통해 공동으로 피해를 예방할 필요성이 인정됨.

□ 신속한 피해 구제를 위하여 금융권은 자체적인 이상금융거래탐지 시스템(FDS³⁾)을 가동하여 사기의심계좌 신속 정지, 피해자 문진·확인 등을 실시 중이나, 금융회사별 정보력·분석역량 편차로 인하여 그 효과가 제한적인 측면이 존재함.

○ 보이스피싱 탐지를 위한 의심정보는 개별 금융회사가 자체 보유한 것이 대부분으로서 타 금융회사와의 정보교류는 매우 제한적

1) 보이스피싱 피해건수: (2023) 1.9만건 → (2024) 2.1만건 (10% ↑)

피해금액: (2023) 4,472억원 → (2024) 8,545억원 (91% ↑)

(2024.1~9.) 5,173억원 → (2025.1~9.) 9,867억원 (90.7% ↑)

2) 한국경제, “[단독] 캄보디아 주목 받자…중국계 범죄조직, 미얀마·라오스로 ‘야반도주’”, 2025. 10. 16. (<https://www.hankyung.com/article/2025101639801>)

3) Fraud Detection System

으로 이루어지고 있고, 관련 정보가 탐지되더라도 단일한 공유 채널이 부재하여 금융회사에 신속한 전파·공유가 어려운 상황임.

- 또한 금융회사별로 의심계좌 탐지 관련 AI 기술 등 개발 수준이 상이하고 관련 인프라·예산 등 자원이 부족한 경우가 있어 최신 수법에 효과적으로 대응하는 데 한계가 존재함.

□ 보이스피싱 범죄 예방을 위한 수단인 ‘계좌 지급정지’ 제도⁴⁾를 보다 효과적으로 활용하기 위하여는 금융·통신·수사 분야의 관련 정보를 신속하고 체계적으로 공유·활용할 수 있도록 제도적 기반을 마련하는 것이 핵심적인 과제라 할 수 있음.

- 금융위원회는 현재 은행권 협조 등을 토대로 「보이스피싱 정보 공유·분석 AI 플랫폼(이하 “ASAP⁵⁾”이라 함)」을 출범(2025. 10. 29.)⁶⁾하여 운영 중이며⁷⁾, 2025년 11월 현재 ASAP에 참여중인

4) 「전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법」 제4조(지급정지) ① 금융회사는 다음 각 호의 어느 하나에 해당하는 경우 거래내역 등의 확인을 통하여 전기통신금융사기의 사기이용계좌로 의심할 만한 사정이 있다고 인정되면 즉시 해당 사기이용계좌의 전부에 대하여 지급정지 조치를 하여야 한다.

1. 제3조제1항에 따른 피해구제 신청이나 같은 조 제2항 또는 제4항에 따른 지급정지 요청이 있는 경우
2. 수사기관 또는 「금융위원회의 설치 등에 관한 법률」에 따라 설립된 금융감독원(이하 “금융감독원”이라 한다) 등으로부터 사기이용계좌로 의심된다는 정보제공이 있는 경우
3. 제2조의5제2항에 따른 피해의심거래계좌에 대한 본인확인조치 결과 사기이용계좌로 추정되는 경우
4. 제15조제3항에 따라 사기이용계좌에 관한 정보를 제공받은 경우
5. 그 밖에 대통령령으로 정하는 경우

5) AI-based anti-phishing Sharing & Analysis Platform: ASAP(에이샵)

금융·통신·수사 과정에서 파악된 보이스피싱 의심정보 등을 참여기관간 실시간으로 공유하고 AI 패턴 분석 등을 통해 범죄를 효과적으로 차단하기 위한 플랫폼

6) 금융보안원은 2016년부터 “이상금융거래정보 공유시스템(FISS)”을 운영하다가, 2025년 이를 고도화하여 “보이스피싱 정보공유·분석 AI 플랫폼(ASAP)”을 출범·운영하고 있음.

(FISS) 공격 및 피해정보, 거래정보, 사기정보(악성앱 등) 공유 / 금융회사만 연동 / 등록된 정보의 단순 공유용으로 활용

금융회사 125개⁸⁾가 총 9개 유형·90개 항목의 정보를 실시간으로 공유·활용하고 있으나, 여전히 금융권 외 통신·수사 분야 정보 활용을 위한 법적 근거가 미흡하여 효과적인 정보 공유 체계를 수립하는 것이 어려운 측면이 있음.

□ 이에 개정안은 전기통신금융사기와 관련된 것으로 의심되는 계좌에 대한 금융·통신·수사 정보 공유 특례를 법제화함으로써, 현재 운영 중인 ASAP이 보이스피싱 범죄 예방에 필요한 보다 광범위한 정보를 제공받아 신속하고 효과적으로 공유·활용하는 체계를 수립하도록 하려는 것임.

○ 개정안 입법 시 보이스피싱 범죄에 활용된 것으로 의심되는 계좌가 포착될 경우 즉시 ASAP을 통해 해당 정보를 공유함으로써 금융회사가 해당 계좌의 출금·이체 등을 차단할 수 있을 것으로 보이며, 중장기적으로는 정보공유 통합 플랫폼 운영을 통해 집중·축적된 금융·통신·수사 정보를 토대로 AI 패턴분석 등을 실시함으로써 전체 참여기관이 공동으로 활용할 수 있는 보이스피싱 탐지 모델을 개발할 수 있을 것으로 기대됨.

(ASAP) 의심계좌 정보, 보이스피싱 관련 해외계좌 정보 등 공유대상 정보 유형 확대 / 금융회사 외 경찰청·통신사 등과도 연동 예정(개정안 입법 시) / AI를 활용한 고도화된 FDS 탐지 모델까지 제공 예정

7) ASAP 운영 관련 보다 상세한 내용은 검토보고 마지막의 [참고2] 자료 참조.

8) 네이버파이낸셜, 다날, 카카오페이 등 전자금융업자 7개 포함

○ 보다 구체적으로, 정보공유 통합 플랫폼의 제도적 기반이 마련될 경우 △단기간 내 다수의 알뜰폰 개통 사실(통신 정보), 악성 앱 설치 명의인 정보(수사 정보) 등을 바탕으로 금융회사가 선제적으로 범죄 의심계좌를 파악해 차단하는 것이 가능해지고, △충분한 AI 인프라를 갖추기 어려운 제2금융권 역시 고도화된 양질의 탐지모델을 기반으로 보이스피싱 범죄를 보다 효과적으로 차단할 수 있게 되며, △해외 거점을 둔 범죄조직의 해외계좌·다발적 이체 등을 활용한 조직적 도피로를 당국이 파악하여 이와 연계된 거래까지 차단·예방하는 것이 용이해질 것으로 전망됨.

3. 주요 내용별 검토

가. 사기관련의심계좌 정의 신설

□ 개정안은 “사기관련의심계좌”의 정의를 전기통신금융사기에 관련된 것으로 의심되는 계좌로서 ① 피해금의 입금·이체·송금·인출에 이용되는 것으로 의심되는 계좌 또는 ② 계좌 명의인에게 피해가 발생할 것으로 의심되는 계좌로 규정하려는 것임(안 제2조제8호 신설).

현 행	개 정 안
제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. 1. ~ 7. (생략) <u><신설></u>	제2조(정의) ----- -----. 1. ~ 7. (현행과 같음) 8. “사기관련의심계좌”란 <u>전기통신금융사기에 관련된 것으로 의심되는 계좌로서 다음 각 목의 어느 하나에 해당하는 계좌를 말한다.</u> <u>가. 피해금의 입금·이체·송금·인출에 이용되는 것으로 의심되는 계좌</u> <u>나. 계좌 명의인에게 피해가 발생할 것으로 의심되는 계좌</u>

□ 현행 「전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법」(이하 “통신사기피해환급법”이라 함)은 전기통신금융사기⁹⁾ 관련 피해의 예방 및 차단을 위한 주요 제도로써 ‘임시조치’ 제도와 ‘지급정지’ 제도를 두고 있음.

○ 임시조치 제도란, 금융회사가 자체점검 또는 타 금융회사로부터 공유받은 정보를 토대로 이용자의 계좌가 전기통신금융사기의 피해를 초래할 수 있는 의심거래계좌(이하 “피해의심거래계좌”라 함)로 이용되는 것으로 추정할 경우, 해당 이용자 계좌의 전부 또는 일부에 대하여 이체, 송금 또는 출금을 지연시키거나 일시 정지하는 제도임¹⁰⁾.

- 임시조치 후에는 지체 없이 이용자에 대한 본인확인조치를 실

9) 「전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법」 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

2. “전기통신금융사기”란 「전기통신기본법」 제2조제1호에 따른 전기통신을 이용하여 타인을 기망(欺罔)·공갈(恐喝)함으로써 자금 또는 재산상의 이익을 취하거나 제3자에게 자금 또는 재산상의 이익을 취하게 하는 다음 각 목의 행위를 말한다. 다만, 재화의 공급 또는 용역의 제공 등을 가장한 행위는 제외하되, 대출의 제공·알선·중개를 가장한 행위는 포함한다.

가. 자금을 송금·이체하도록 하는 행위

나. 개인정보를 알아내어 자금을 송금·이체하는 행위

다. 자금을 교부받거나 교부하도록 하는 행위

라. 자금을 출금하거나 출금하도록 하는 행위

10) 「전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법」 제2조의5(이용자계좌에 대한 임시조치) ① 금융회사는 다음 각 호의 어느 하나에 해당하는 경우 해당 이용자 계좌의 전부 또는 일부에 대하여 이체, 송금 또는 출금을 지연시키거나 일시 정지하는 조치(이하 “임시조치”라 한다)를 하여야 한다.

1. 대통령령으로 정하는 절차에 따라 자체점검을 상시적으로 실시하여 이용자의 계좌가 전기통신금융사기의 피해를 초래할 수 있는 의심거래계좌(이하 “피해의심거래계좌”라 한다)로 이용되는 것으로 추정할 만한 사정이 있다고 인정되는 경우

2. 제15조제3항에 따라 이용자의 계좌가 피해의심거래계좌로 추정된다는 정보를 제공받은 경우

② 금융회사는 제1항에 따라 임시조치를 한 경우 지체 없이 해당 이용자에게 임시조치에 관한 사항을 통지하고 본인확인조치를 하여야 한다.

③ 금융회사는 제2항에 따른 본인확인조치 결과 해당 이용자의 계좌가 피해의심거래계좌에 해당하지 아니하는 경우에는 제1항에 따른 임시조치를 해제하여야 한다.

시하고, 피해의심거래계좌에 확인하지 않는다는 점이 확인될 경우 즉시 임시조치를 해제하여야 함.

○ **지급정지** 제도란, 금융회사가 △피해자의 요청, △자체점검, △수사기관·금융감독원·타 금융회사로부터의 사기 의심정보를 제공받은 경우 거래내역 등을 확인한 후 사기이용계좌¹¹⁾로 의심할 만한 사정이 있다고 인정되면 즉시 해당 사기이용계좌의 전부에 대하여 입출금·이체 등 모든 거래를 중단시키는 제도임¹²⁾.

- 지급정지 후에는 금융감독원에서 해당 계좌 명의인에 대한 채권소멸절차를 개시하고, 채권소멸절차 개시 공고 후 2개월이 경과하면 채권이 소멸하며, 금융감독원은 채권이 소멸된 날부터 14일 이내에 피해환급금 지급 대상 및 금액을 결정하여 금융회사가 피해자에게 피해환급금을 지급하도록 함¹³⁾.

11) 「전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법」 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

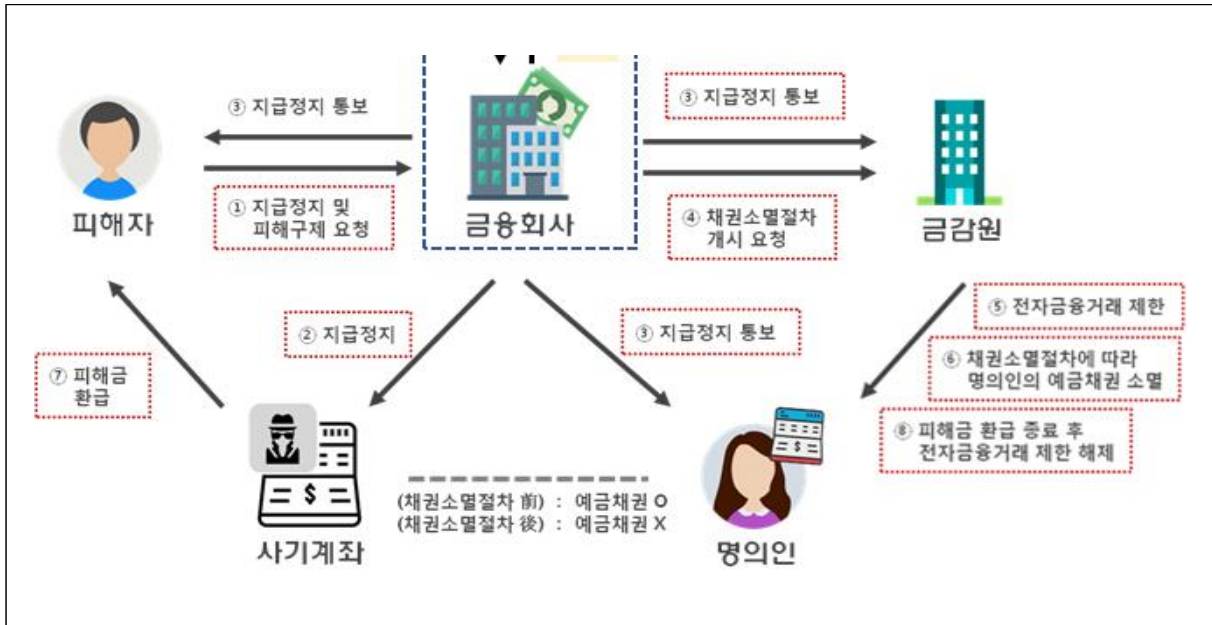
4. “사기이용계좌”란 전기통신금융사기로 인하여 피해자의 자금이 송금·이체된 계좌, 피해자가 교부하였거나 피해자의 계좌에서 출금된 자금이 입금된 계좌 및 해당 계좌로부터 자금의 이전에 이용된 계좌를 말한다.

12) 「전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법」 제4조(지급정지) ① 금융회사는 다음 각 호의 어느 하나에 해당하는 경우 거래내역 등의 확인을 통하여 전기통신금융사기의 사기이용계좌로 의심할 만한 사정이 있다고 인정되면 즉시 해당 사기이용계좌의 전부에 대하여 지급정지 조치를 하여야 한다.

1. 제3조제1항에 따른 피해구제 신청이나 같은 조 제2항 또는 제4항에 따른 지급정지 요청이 있는 경우
2. 수사기관 또는 「금융위원회의 설치 등에 관한 법률」에 따라 설립된 금융감독원(이하 “금융감독원”이라 한다) 등으로부터 사기이용계좌로 의심된다는 정보제공이 있는 경우
3. 제2조제5제2항에 따른 피해의심거래계좌에 대한 본인확인조치 결과 사기이용계좌로 추정되는 경우
4. 제15조제3항에 따라 사기이용계좌에 관한 정보를 제공받은 경우
5. 그 밖에 대통령령으로 정하는 경우

13) 지급정지된 계좌의 명의인은 지급정지, 전자금융거래 제한 및 채권소멸절차에 대하여 이의가 있을 경우 금융회사에 이의를 제기할 수 있으며, 금융회사는 해당 계좌가 사기이용계좌가 아니라는 사실이 소명된 경우 등에는 지급정지 등을 종료하여야 함.

[통신사기피해환급법상 지급정지 절차¹⁴⁾]



(자료: 금융위원회)

□ 개정안은 현재 운영중인 전기통신금융사기 피해자 구제 제도를 보다 효과적으로 운영하기 위하여 금융·통신·수사 분야의 정보를 집중·공유하기 위한 통합플랫폼을 구축하는 것을 골자로 하는데, 이를 위하여 안 제2조제8호에서 “사기관련의심계좌”의 정의를 신설하고, 사기관련의심계좌의 거래내역 및 명의인에 관한 정보를 해당 플랫폼에서 수집·공유할 수 있도록 근거를 마련¹⁵⁾하려는 것임.

○ 현행법 제15조제3항은 금융회사 및 전자금융업자로 하여금 사기 이용계좌¹⁶⁾와 피해의심거래계좌¹⁷⁾에 관한 정보를 서로 공유하

14) 지급정지 제도 등 보다 상세한 내용은 검토보고 마지막의 [참고1] 자료 참조.

15) 정보공유 관련 규정은 신설조항인 안 제13조의4에 반영되어 있음.

16) 전기통신금융사기로 인하여 피해자의 자금이 송금·이체된 계좌, 피해자가 교부하였거나 피해자의 계좌에서 출금된 자금이 입금된 계좌 및 해당 계좌로부터 자금의 이전에 이용된 계좌(법 제2조제4호)

17) 전기통신금융사기의 피해를 초래할 수 있는 의심거래계좌(법 제2조의5제1항제1호)

도록 규정하고 있는바¹⁸⁾, 피해자로부터 피해금이 인출·출금되는 계좌, 즉 피해자의 계좌에 대한 정보는 공유 대상으로 규정되어 있지 않음.

- 반면, 개정안에서 정의하려는 ‘사기관련의심계좌’의 범위에는 피해금이 입금·이체·송금·인출되는 것으로 의심되는 계좌, 즉 계좌 명의인이 보이스피싱 범죄자일 것으로 의심되는 계좌뿐만 아니라 계좌 명의인에게 피해가 발생할 것으로 의심되는 계좌까지 포함됨.
- 개정안에 따르면 전기통신금융사기 범죄 관련 자금 흐름을 추적하기 위해 필요한 관련 계좌가 모두 정보공유 플랫폼에 집중·공유될 수 있는바, 관련 의심정보 및 피해가능성을 선제적으로 파악하고 대응하는 데 기여할 수 있을 것으로 예상됨.

18) 「전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법」 제15조(계좌자료 제공 등에 대한 특례) ③ 금융회사 및 「전자금융거래법」 제2조제4호에 따른 전자금융업자로서 대통령령으로 정하는 자는 「금융실명거래 및 비밀보장에 관한 법률」 제4조, 「신용정보의 이용 및 보호에 관한 법률」 제32조·제33조 및 「전자금융거래법」 제26조에도 불구하고 전기통신금융사기의 사기이용계좌와 피해의심거래계좌에 관한 정보를 대통령령으로 정하는 바에 따라 서로 공유하여야 한다.

나. 전기통신금융사기 관련 정보공유 체계 수립

□ 개정안은 금융위원회가 전기통신금융사기에 관한 정보를 제공받아 분석하여 공유하는 기관(이하 “정보공유분석기관”이라 함)을 지정하여 고시하도록 하고(안 제13조의4제1항 신설),

정보공유분석기관에 정보주체의 동의 없이 전기통신금융사기 관련 정보를 제공하는 기관(이하 “사기정보제공기관”이라 함)을 금융기관, 전기통신사업자, 수사기관, 그 밖에 대통령령으로 정하는 자로 규정하며, 정보공유분석기관이 제공받았거나 자체적으로 분석·생성한 정보를 정보주체의 동의 없이 제공할 수 있는 기관(이하 “사기정보이용기관”이라 함)을 금융기관, 그 밖에 대통령령으로 정하는 자로 규정하려는 것임(안 제13조의4제2항 및 제3항 신설).

○ 또한 사기정보제공기관이 정보공유분석기관에게 정보주체의 동의 없이 전기통신금융사기 관련 정보를 제공하는 것을 **재량**으로 규정하되(안 제13조의4제1항), 그 중에서도 전기통신금융사기의 분석·대응에 필수적인 정보로서 대통령령으로 정하는 정보의 제공을 정보공유분석기관이 사기정보제공기관에게 요청하는 경우 이를 **의무**적으로 제공하도록 규정하려는 것임(안 제13조의4제2항 신설).

○ 그리고 사기정보이용기관 및 정보공유분석기관이 제공받은 정보를 정보주체의 동의 없이 처리할 수 있는 근거를 마련하고, 이 경우 정보공유분석기관은 업무 수행을 위해 불가피한 경우 고유식별정보를 처리할 수 있도록 하려는 것임(안 제13조의4제4항 신설).

현 행	개 정 안
<u><신 설></u>	제13조의4(전기통신금융사기 정보의 공유 등) ① 금융회사, 전기통신사업자(「전기통신사업법」 제2조제8호에 따른 전기통신사업자를 말한다. 이하 같다), 수사기관, 그 밖에 대통령령으로 정하는 자(이하 이 조에서 “<u>사기정보제공기관</u>”이라 한다)는 전기통신금융사기의 예방 및 피해 확산 방지를 위하여 전기통신금융사기에 관한 정보로서 다음 각 호의 정보를 전기통신금융사기 정보공유분석기관(전기통신금융사기에 관한 정보를 제공받아 분석하여 공유하는 기관으로서 금융위원회가 지정하여 고시하는 기관을 말한다. 이하 “<u>정보공유분석기관</u>”이라 한다)에 정보주체의 동의를 받지 아니하고 제공할 수 있다. 1. 피해발생계좌, 사기이용계좌 및 사기관련의심계좌와 그 계좌의 거래내역 및 명의인에 관한 정보로서 대통령령으로 정하는 정보 2. 전기통신금융사기에 이용되거나 이용된 것으로 의심되는 「전기통신사업법」에 따른 전기통신번호·단말기기·이동통신단말장치와 관련된 정보통신서비스 이용계약의 내용 및 그 이용자에 관한 정보로서 대통령령으로 정하는 정보 3. 전기통신금융사기를 위하여 「개인정보 보호법」 제2조제1호에 따른 개인정보, 「전자금융거래법」 제2조제10호에 따른 접근매체 또는 같은 조 제1호에 따른 전자금융거래의 진실성과 정확성을 확보하기 위하여 사용되는 매체·수단에 관한 정보(이하 이 호에서 “<u>개인정보등</u>”이라 한다)을 수집하는 데 이용되거나 이용된 것으로 의심되는 인터넷홈페이지, 응용프로그램, 이동통신단말장치에서 사용되는 애플리케이션(Application) 및 이를 통해 개인정

보통이 유출된 자(유출된 것으로 의심되거나 유출될 가능성이 현저히 높은 경우를 포함한다)에 관한 정보로서 대통령령으로 정하는 정보

4. 그 밖에 전기통신금융사기의 예방 및 피해 확산 방지를 위해 필요한 정보로서 대통령령으로 정하는 정보

② 제1항에도 불구하고 사기정보제공기관은 정보공유분석기관으로부터 제1항 각 호의 정보 중에서 전기통신금융사기의 분석·대응에 필수적인 정보로서 대통령령으로 정하는 정보의 제공을 요청받은 경우에는 정당한 사유가 없는 한 이에 따라야 한다.

③ 정보공유분석기관은 제1항 및 제2항에 따라 사기정보제공기관으로부터 제공받거나 자신이 분석·생성한 정보로서 전기통신금융사기의 예방 및 피해 확산 방지에 필요한 정보를 금융회사, 그 밖에 대통령령으로 정하는 자(이하 “사기정보이용기관”이라 한다)에게 정보주체의 동의를 받지 아니하고 제공할 수 있다.

④ 사기정보이용기관 및 정보공유분석기관은 전기통신금융사기의 예방 및 피해 확산을 방지에 관한 업무를 수행하기 위한 목적으로 제1항부터 제3항까지에 따라 제공받은 정보를 정보주체의 동의를 받지 아니하고 처리할 수 있다. 이 경우 정보공유분석기관은 해당 업무를 수행하기 위하여 불가피한 경우에 사기정보제공기관으로부터 「개인정보 보호법」 제24조에 따른 고유식별정보(같은 법 제24조의2에 따른 주민등록번호를 포함한다)를 제공받아 처리할 수 있다.

⑧ 제1항부터 제4항까지에 따른 정보의 제공 및 처리, 정보공유분석기관의 지정의 요건 및 절차, 지정의 취소 등에 필요한 사항은 대통령령으로 정한다.

□ 현행 「통신사기피해환급법」에 따라 금융회사 상호 간에는 사기이용계좌 및 피해의심거래계좌에 관한 정보를 공유할 수 있음¹⁹⁾.

○ 반면, 금융회사가 해당 정보를 금융회사가 아닌 금융보안원²⁰⁾에 집중적으로 제공하여 공유·활용할 수 있는지에 대하여는 명시적인 법적 근거가 없는 상황으로, 금융위원회의 「금융실명거래 및 비밀보장에 관한 법률」 유권해석²¹⁾에 근거하여 금융보안원의 보이스포싱 정보공유·분석 AI 플랫폼(ASAP)이 제한적으로²²⁾ 운영되고 있음.

19) 「전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법」 제15조(계좌자료 제공 등에 대한 특례) ③ 금융회사 및 「전자금융거래법」 제2조제4호에 따른 전자금융업자로서 대통령령으로 정하는 자는 「금융실명거래 및 비밀보장에 관한 법률」 제4조, 「신용정보의 이용 및 보호에 관한 법률」 제32조·제33조 및 「전자금융거래법」 제26조에도 불구하고 전기통신금융사기의 사기이용계좌와 피해의심거래계좌에 관한 정보를 대통령령으로 정하는 바에 따라 서로 공유하여야 한다.

20) 민법 제32조에 따라 설립된 비영리사단법인

- 2015년 대형 금융보안사고 방지 및 전자금융사기 예방·대응 등을 위한 금융보안 전담기구로서 설립되었으며, 현재 ASAP의 운영 주체임.

21) 금융위원회의 「금융실명법」 유권해석:

이상금융거래 정보 중 「금융실명법」상 금융거래정보는 금융범죄 방지 목적의 금융사고 관련 정보로서 금융회사 상호간의 업무상 필요한 거래정보에 해당하므로, 법 제4조제1항제5호에 의거하여 서면 동의 없이 제3자 제공이 가능함.

※ 참고로 해당 유권해석은 ASAP의 전신인 금융보안원의 이상금융거래정보 공유시스템(FISS) 운영례에 대한 해석이나, ASAP에 대해서도 동일한 해석을 적용할 수 있을 것으로 보임.

「금융실명거래 및 비밀보장에 관한 법률」 제4조(금융거래의 비밀보장) ① 금융회사등에 종사하는 자는 명의인(신탁의 경우에는 위탁자 또는 수익자를 말한다)의 서면상의 요구나 동의를 받지 아니하고는 그 금융거래의 내용에 대한 정보 또는 자료(이하 “거래정보등”이라 한다)를 타인에게 제공하거나 누설하여서는 아니 되며, 누구든지 거짓 또는 그 밖의 부정한 수단이나 방법으로 금융회사등에 종사하는 자에게 거래정보등의 제공을 요구하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우로서 그 사용 목적에 필요한 최소한의 범위에서 거래정보등을 제공하거나 그 제공을 요구하는 경우에는 그러하지 아니하다.

5. 동일한 금융회사등의 내부 또는 금융회사등 상호간에 업무상 필요한 거래정보등의 제공

22) ASAP의 전신이 되는 FISS의 경우 「개인정보 보호법」 등 기타 법령의 저촉 여부가 명확하게 해소되지 않는 측면이 있어 이용률이 저조하였으며, ASAP 역시 FISS와 동일한 제도적 한계를 지니고 있음.

연도별 FISS* 이상금융거래정보 공유건수 (2022년) 184건 → (2023년) 259건 → (2024년) 193건
(* 2025년 10월 기준 FISS를 고도화한 ASAP 출범)

○ 또한 금융권 외에 경찰 등 수사기관이나 통신사가 업무 과정에서 수집·탐지한 보이스피싱 의심 정보를 금융권과 공유·활용할 수 있는지에 대한 법적 근거 역시 미비한 상황임.

- 통신 관련 정보의 경우 별도의 정보공유 근거가 부재하여 현재 금융권과의 공유·활용이 이루어지지 않고 있는 상황이고²³⁾, 수사 관련 정보의 경우 악성 앱 설치자 관련 정보 등 경찰청에서 수집하는 일부 정보만이 개인정보보호위원회의 「개인정보 보호법」 유권해석²⁴⁾에 근거하여 금융회사에 제한적으로 제공·공유되고

23) 다만, 통신사와 개별 금융회사 간의 계약을 통해 정보주체의 동의를 얻어 일부 정보를 제공·수신 중인 상황임.

24) 개인정보보호위원회의 「개인정보 보호법」 유권해석:

(1) 악성 앱 설치자의 '성명'을 금융기관에 제공하는 것은 당초 수집한 목적 범위를 초과하여 제3자에 제공하는 것에 해당하나, 보이스피싱 조직에 의하여 악성 앱을 설치한 자의 재산을 보호하고 범죄를 예방하는 것은 경찰청의 법률상 소관업무에 해당하고, 설치자의 성명 제공이 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있다고 보기 어려우므로 「개인정보 보호법」 제18조제2항제5호에 따라 목적 외로 제3자에게 제공할 수 있음.

(2) 악성 앱 설치자의 '주민등록번호'를 금융기관에 제공하는 것은 「경찰관 직무집행법 시행령」 제8조에 근거하여, 경찰관 직무 수행을 위하여 불가피한 경우 가능함.

「개인정보 보호법」 제18조(개인정보의 목적 외 이용·제공 제한) ① 개인정보처리자는 개인정보를 제15조제1항에 따른 범위를 초과하여 이용하거나 제17조제1항 및 제28조의8제1항에 따른 범위를 초과하여 제3자에게 제공하여서는 아니 된다.

② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 다만, 제5호부터 제9호까지에 따른 경우는 공공기관의 경우로 한정한다.

5. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우

제24조의2(주민등록번호 처리의 제한) ① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.

1. 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우

「경찰관 직무집행법 시행령」(대통령령 제34891호, 2024. 9. 19., 일부개정 → 참고로 해당 조문은 현재 삭제되었으나, 2024. 12. 3. 제정된 「경찰공무원 등의 개인정보 처리에 관한 규정」에 해당 내용이 반영됨) 제8조(민감정보 및 고유식별정보의 처리) 경찰관은 법 제2조에 따른 경찰관의 직무를 수행하기 위하여 불가피한 경우 「개인정보 보호법」 제23조에 따른 건강에 관한 정보, 같은 법 시행령 제18조제2호에 따른 범죄경력자료에 해당하는 정보, 같은 영 제19조에 따른 주민등록

있는 실정임.

□ 이에 개정안은 정보공유분석기관을 중심으로 금융·통신·수사 기관 모두가 전기통신금융사기 관련 의심정보를 집중·제공하도록 하여, 금융회사 등 사기정보이용기관이 해당 정보를 전기통신금융사기의 예방 및 피해 확산 방지에 활용하도록 근거를 마련하려는 긍정적인 입법조치로 보임.

○ 구체적으로, 개정안에 따라 정보공유분석기관에서 제공받아 공유하게 되는 정보 현황은 다음과 같으며, 이 중 안 제13조의4제1항제2호에 규정된 정보항목의 경우 현재 운영중인 ASAP에서 공유·관리하고 있지 않은 통신 관련 정보로서, 개정안 입법 시 비로소 원활한 제공·활용이 가능해질 것으로 보임.

록번호, 여권번호, 운전면허의 면허번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다.

[개정안에 따라 정보공유분석기관에 집중·공유되는 정보 현황]

개정안 제13조의4	정보항목
①-1 (피해발생계좌, 사기이용계좌 및 사기관련의 심계좌와 그 계좌의 거래내역 및 명의인에 관한 정보)	▪ 피해 계좌 정보 ▪ 사기이용 계좌 정보 ▪ 의심 계좌 정보 ▪ 보이스피싱이용 해외계좌 정보 ▪ 보이스피싱 피해의심자 정보
①-2 (전기통신금융사기에 이용되거나 이용된 것으로 의심되는 전기통신번호·단말기기·이동통신단말장치와 관련된 정보통신서비스 이용계약의 내용 및 그 이용자에 관한 정보)	▪ 명의자의 통신사별 개통 회선 수 ▪ 개통된 회선의 개통일로부터 경과 기간 ▪ 개통된 회선의 알뜰폰 여부 ▪ 개통된 회선의 선불/후불 여부
①-3 (개인정보 등을 수집하는 데 이용되거나 이용된 것으로 의심되는 인터넷홈페이지, 응용프로그램, 이동통신단말장치에서 사용되는 애플리케이션(Application) 및 이를 통해 개인정보등이 유출된 자에 관한 정보)	▪ 피싱사이트 탐지 정보 ▪ 악성앱 탐지 정보
①-4 (그 밖에 전기통신금융사기의 예방 및 피해 확산 방지를 위해 필요한 정보)	▪ 기타 사고·의심 정보 ▪ 위조신분증 정보
② (제1항 각 호의 정보 중에서 전기통신금융사기의 분석·대응에 필수적인 정보)	▪ 피해 계좌 정보 ▪ 사기이용 계좌 정보 ▪ 악성앱 탐지 정보 ▪ 기타 사고·의심 정보

주: 이탤릭(굵은글씨) 표시된 정보항목은 전기통신금융사기의 분석·대응에 필수적인 정보를 의미함.
(자료: 금융위원회)

□ 「개인정보 보호법」 제18조²⁵⁾는 개인정보처리자가 개인정보를 수집한 목적 범위를 초과하여 이용하거나 제3자에 제공하는 것을 원칙적으로 금지하면서(제1항), 예외적으로 △정보주체의 동의를 받았거나 △다른 법률에 특별한 규정이 있는 경우 등에는 정보주체나 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고 해당 개인정보를 목적 범위를 초과하여 이용·제공할 수 있도록 하고 있음(제2항).

○ 개정안 제13조의4제1항 및 제2항은 사기정보제공기관²⁶⁾이 고유한 업무 목적으로 수집한 정보를 정보공유분석기관에게 제공하도록 하고 있는바, 이는 사기정보제공기관이 당초 정보를 수집한 목적 범위를 초과하여 제3자에 제공하는 것에 해당하나, 이는 「개인정보 보호법」 제18조제2항제2호에 따라 ‘다른 법률에 특별한 규정이 있는 경우’에 해당함. 또한 이러한 제3자 제공의 목적은 전기통신금융사기의 예방 및 피해 확산 방지를 위한 것

25) 「개인정보 보호법」 제18조(개인정보의 목적 외 이용·제공 제한) ① 개인정보처리자는 개인정보를 제15조제1항에 따른 범위를 초과하여 이용하거나 제17조제1항 및 제28조의8제1항에 따른 범위를 초과하여 제3자에게 제공하여서는 아니 된다.

② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 다만, 제5호부터 제9호까지에 따른 경우는 공공기관의 경우로 한정한다.

1. 정보주체로부터 별도의 동의를 받은 경우
2. 다른 법률에 특별한 규정이 있는 경우
3. 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
5. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우
6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
8. 법원의 재판업무 수행을 위하여 필요한 경우
9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우
10. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우

26) 금융회사, 전기통신사업자, 수사기관, 그 밖에 대통령령으로 정하는 자

으로서 정보주체의 실질적 이익을 부당하게 침해한다고 보기 어려울 것으로 보임.

○ 한편 개정안 제13조의4제4항 전단은 사기정보이용기관 및 정보공유분석기관이 전기통신금융사기의 예방 및 피해 확산을 방지에 관한 업무를 수행하기 위한 목적으로 제공받은 정보를 정보주체의 동의 없이 처리할 수 있도록 규정하고 있는데, 이는 제공받은 목적 범위 내 이용이므로 법 체계상 문제가 없을 것으로 보이며²⁷⁾, 보이스피싱 범죄 예방 등의 목적이라는 점에서 타당한 입법조치로 생각됨.

○ 그리고 개정안 제13조의4제4항 후단은 정보공유분석기관이 업무 수행에 불가피한 경우 사기정보제공기관으로부터 고유식별정보(주민등록번호를 포함)를 제공받아 처리할 수 있도록 규정하고 있는데, 이는 「개인정보 보호법」상 법률에서 구체적으로 고유식별정보·주민등록번호의 처리를 허용한 경우에 해당하므로 법 체계상 문제가 없는 것으로 보이고²⁸⁾, 이 역시 입법정책적으로 필요한 조치로 보임.

27) 「개인정보 보호법」 제15조(개인정보의 수집·이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.

1. 정보주체의 동의를 받은 경우
 2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
 3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
- (이하 각 호 생략)

제19조(개인정보를 제공받은 자의 이용·제공 제한) 개인정보처리자로부터 개인정보를 제공받은 자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 개인정보를 제공받은 목적 외의 용도로 이용하거나 이를 제3자에게 제공하여서는 아니 된다.

1. 정보주체로부터 별도의 동의를 받은 경우
2. 다른 법률에 특별한 규정이 있는 경우

- 참고로, 안 제4항 후단은 고유식별정보(주민등록번호 포함)를 처리할 수 있는 주체를 정보공유분석기관으로 한정하여 규정하고 사기정보이용기관은 포함하고 있지 않은데, 이는 사기정보이용기관 중 금융회사의 경우 「금융실명거래 및 비밀보장에 관한 법률 시행령」²⁹⁾ 등에 관련 처리 근거가 마련되어 있기 때문이다.
- 또한 사기정보이용기관의 범위는 추후 시행령을 통해 연구기관, 보안업체 등을 포괄하여 규정될 가능성이 있는데, 만일 개정안에서 정보공유분석기관 외에 사기정보이용기관도 고유식별정보를 처리할 수 있도록 일률적으로 규정할 경우 고유식별정보를 처리할 수 있는 대상기관의 범위가 과도하게 확대될 우려가 있는바, 이를 정보공유분석기관으로 제한한 개정내용은 타당한 것으로 보임.

28) 「개인정보 보호법」 제24조(고유식별정보의 처리 제한) ① 개인정보처리자는 다음 각 호의 경우를 제외하고는 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보(이하 “고유식별정보”라 한다)를 처리할 수 없다.

1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우

제24조의2(주민등록번호 처리의 제한) ① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.

1. 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 보호위원회가 고시로 정하는 경우

29) 「금융실명거래 및 비밀보장에 관한 법률 시행령」 제4조의2(실명거래의 확인 등) ① 금융거래를 할 때 실지명의를 다음 각 호의 구분에 따른 증표·서류에 의하여 확인한다.

1. 개인의 경우
 - 가. 주민등록증 발급대상자는 주민등록증(모바일 주민등록증을 포함한다). 다만, 주민등록증(모바일 주민등록증을 포함한다)에 의하여 확인하는 것이 곤란한 경우에는 국가기관, 지방자치단체 또는 「교육기본법」에 따른 학교의 장이 발급한 것으로서 실지명의를 확인이 가능한 증표 또는 주민등록번호를 포함한 주민등록표 초본과 신분을 증명할 수 있는 증표에 의하여 확인한다.
 - 나. 주민등록증 발급대상자가 아닌 자는 주민등록번호를 포함한 주민등록표 초본과 법정대리인의 가목의 증표 또는 실지명의를 확인이 가능한 증표·서류
 - 다. 재외국민은 제3조제1호 단서에 따른 여권 또는 재외국민등록증

- 또한 개정안에 따르면 ‘사기정보제공기관’과 ‘사기정보이용기관’의 규정범위가 상이한바, 사기정보제공기관의 범위에는 금융회사 뿐만 아니라 ‘전기통신사업자, 수사기관’을 명시적으로 포함시킨 반면 사기정보이용기관의 범위에서는 해당 기관들이 포함되어 있지 않음.
- 이는 정보공유분석기관에 정보를 제공하는 기관의 범위는 가급적 폭넓게 규정하여 전기통신금융사기 관련 의심정보를 최대한 집중할 수 있도록 하되, 다만 해당 정보를 제공받아 활용할 수 있는 기관의 범위는 금융회사 등 제한적으로 규정함으로써 개인정보의 오·남용 등 우려를 최소화하기 위한 취지로 보임.

[사기정보제공기관과 사기정보이용기관의 규정범위 비교]

구 분	개정안의 규정내용
사기정보제공기관	금융회사, 전기통신사업자, 수사기관, 그 밖에 대통령령으로 정하는 자
사기정보이용기관	금융회사, 그 밖에 대통령령으로 정하는 자

- 추가적으로, 안 제13조의4제1항제1호 중 ‘피해발생계좌’는 피해금이 인출된 피해자의 계좌를 의미하는 것으로 보이는데, 해당 의미를 보다 명확히 하기 위해 이를 ‘전기통신금융사기로 인하여 피해자의 자금이 출금·인출된 계좌’ 또는 ‘피해자의 계좌’ 등으로 풀어쓰는 방안을 고려할 필요가 있음.

다. 전기통신금융사기 관련 정보의 공유·처리 관련 안전조치

- 개정안은 정보공유분석기관으로 하여금 전기통신금융사기 관련 정보 처리에 관하여 △해당 정보가 분실·유출 등 되지 아니하고 △정보처리시스템에 대한 제3자의 불법적인 접근 등에 대하여 안전성을 확보할 수 있도록 기술적·물리적·관리적 대책을 수립·시행하도록 하고(안 제13조의4제5항 신설),
- 사기정보제공기관, 사기정보이용기관 및 정보공유분석기관으로 하여금 관련 정보 처리 시 준수하여야 할 사항을 규정하려는 것임(안 제13조의4제7항 신설).

현 행	개 정 안
<신 설>	제13조의4(전기통신금융사기 정보의 공유 등) ⑤ 정보공유분석기관은 전기통신금융사기에 관한 정보의 처리에 관하여 해당 정보가 분실·도난·유출·위조·변조·훼손되지 아니하고 해당 정보를 처리하는 정보처리시스템에 대한 제3자의 불법적인 접근 또는 그 밖의 위험에 대하여 안전성을 확보할 수 있도록 대통령령으로 정하는 바에 따라 기술적·물리적·관리적 대책을 수립·시행하여야 한다. ⑦ 사기정보제공기관, 사기정보이용기관 및 정보공유분석기관은 제1항부터 제4항까지의 규정에 따라 정보를 처리하는 경우에는 다음 각 호의 사항을 준수하여야 한다. 1. 해당 정보를 전기통신금융사기의 예방 및 피해 확산을 방지하기 위한 목적 외의 목적으로 이용하지 않을 것 2. 제공받은 정보가 제공받은 날부터 5년의 범위 안에서

	<u>대통령령으로 정하는 기간이 경과한 때에는 대통령령으로 정하는 바에 따라 해당 정보를 파기 또는 삭제할 것</u> <u>3. 정보주체가 대통령령으로 정하는 바에 따라 정보를 제공하거나 제공받은 사실을 조회할 수 있도록 할 것</u> <u>4. 그 밖에 전기통신금융사기의 예방, 피해 확산 방지 및 개인·신용·금융거래에 관한 정보의 안전한 관리를 위하여 필요한 사항으로서 대통령령으로 정하는 사항</u>
--	---

□ 「개인정보 보호법」 제29조³⁰⁾는 개인정보처리자로 하여금 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하도록 규정하고 있음.

○ 개정안 제13조의4제5항은 「개인정보 보호법」의 규정과는 별개로 「통신사기피해환급법」에 정보공유분석기관의 안전성 확보를 위한 기술적·물리적·관리적 대책 수립 의무를 부과하려는 것으로, 「개인정보 보호법」의 내용과 중복되는 측면은 있으나 전기통신금융사기 관련 정보의 안전성 확보를 강조하는 취지에서 유사한 내용을 규정한 것이고, 전기통신금융사기 분야에 특화된 사항을 정할 수 있을 것으로 보이므로 특별한 문제는 없는 것으로 생각됨.

30) 「개인정보 보호법」 제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

라. 개별법상 정보보호 규정 관련 특례

- 개정안은 사기정보제공기관, 사기정보이용기관 및 정보공유분석기관이 정보공유분석기관을 통해 전기통신금융사기 관련 정보를 처리하는 경우 「금융실명거래 및 비밀보장에 관한 법률」 제4조 및 제4조의2, 「신용정보의 이용 및 보호에 관한 법률」 제32조, 제35조 및 제38조 및 그 밖에 제1호 및 제2호와 유사한 법률의 규정으로서 대통령령으로 정하는 법률의 규정의 적용을 제외하려는 것임 (안 제13조의4제6항 신설).

현 행	개 정 안
<신 설>	제13조의4(전기통신금융사기 정보의 공유 등) ⑥ 사기정보제공기관, 사기정보이용기관 및 정보공유분석기관이 제1항부터 제4항까지의 규정에 따라 정보를 처리하는 경우에는 다음 각 호의 규정을 적용하지 아니한다. 1. 「금융실명 거래 및 비밀보장에 관한 법³¹⁾」 제4조 및 제4조의2 2. 「신용정보의 이용 및 보호에 관한 법률」 제32조, 제35조 및 제38조 3. 그 밖에 제1호 및 제2호와 유사한 법률의 규정으로서 대통령령으로 정하는 법률의 규정

31) 법률의 공식 제명은 “금융실명거래 및 비밀보장에 관한 법률”로, 입법 시 수정이 필요함.

□ 「금융실명거래 및 비밀보장에 관한 법률」 제4조 및 제4조의2³²⁾는 금융회사등 종사자가 명의인의 동의 없이 거래정보등을 타인에게 제공하는 것을 금지하고, 예외적으로 사용 목적에 필요한 최소한의 범위에서 거래정보등을 제공하는 것을 허용함. 또한 명의인의 동의를 받아 거래정보등을 제공한 경우 등에 해당 제공사실 등을 명의인에게 통보하도록 규정함.

○ 또한 「신용정보의 이용 및 보호에 관한 법률」 제32조, 제35조 및 제38조³³⁾는 신용정보제공·이용자가 개인신용정보를 타인에

32) 「금융실명거래 및 비밀보장에 관한 법률」 제4조(금융거래의 비밀보장) ① 금융회사등에 종사하는 자는 명의인(신탁의 경우에는 위탁자 또는 수익자를 말한다)의 서면상의 요구나 동의를 받지 아니하고는 그 금융거래의 내용에 대한 정보 또는 자료(이하 “거래정보등”이라 한다)를 타인에게 제공하거나 누설하여서는 아니 되며, 누구든지 거짓 또는 그 밖의 부정한 수단이나 방법으로 금융회사등에 종사하는 자에게 거래정보등의 제공을 요구하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우로서 그 사용 목적에 필요한 최소한의 범위에서 거래정보등을 제공하거나 그 제공을 요구하는 경우에는 그러하지 아니하다.

1. 법원의 제출명령 또는 법관이 발부한 영장에 따른 거래정보등의 제공
(이하 각 호 생략)

제4조의2(거래정보등의 제공사실의 통보) ① 금융회사등은 명의인의 서면상의 동의를 받아 거래정보등을 제공한 경우나 제4조제1항제1호·제2호(조세에 관한 법률에 따라 제출의무가 있는 과세자료 등의 경우는 제외한다)·제3호 및 제8호에 따라 거래정보등을 제공한 경우에는 제공한 날(제2항 또는 제3항에 따라 통보를 유예한 경우에는 통보유예기간이 끝난 날)부터 10일 이내에 제공한 거래정보등의 주요 내용, 사용 목적, 제공받은 자 및 제공일 등을 명의인에게 서면으로 통보하여야 한다.

33) 「신용정보의 이용 및 보호에 관한 법률」 제32조(개인신용정보의 제공·활용에 대한 동의) ① 신용정보제공·이용자가 개인신용정보를 타인에게 제공하려는 경우에는 대통령령으로 정하는 바에 따라 해당 신용정보주체로부터 다음 각 호의 어느 하나에 해당하는 방식으로 개인신용정보를 제공할 때마다 미리 개별적으로 동의를 받아야 한다. (단서 및 각 호 생략)

제35조(신용정보 이용 및 제공사실의 조회) ① 신용정보회사등은 개인신용정보를 이용하거나 제공한 경우 대통령령으로 정하는 바에 따라 다음 각 호의 구분에 따른 사항을 신용정보주체가 조회할 수 있도록 하여야 한다. 다만, 내부 경영관리의 목적으로 이용하거나 반복적인 업무위탁을 위하여 제공하는 경우 등 대통령령으로 정하는 경우에는 그러하지 아니하다.

1. 개인신용정보를 이용한 경우: 이용 주체, 이용 목적, 이용 날짜, 이용한 신용정보의 내용, 그 밖에 대통령령으로 정하는 사항
2. 개인신용정보를 제공한 경우: 제공 주체, 제공받은 자, 제공 목적, 제공한 날짜, 제공한 신용정보의 내용, 그 밖에 대통령령으로 정하는 사항

제38조(신용정보의 열람 및 정정청구 등) ① 신용정보주체는 신용정보회사등에 본인의 신분을

게 제공하려는 경우 해당 신용정보주체로부터 개인신용정보를 제공할 때마다 미리 개별적으로 동의를 받도록 하고, 신용정보회사등이 개인신용정보를 이용하거나 제공한 경우 이용·제공 관련 사실을 신용정보주체가 조회할 수 있도록 하며, 신용정보주체가 본인 확인 후 신용정보회사등에게 본인에 관한 신용정보의 교부 또는 열람을 청구할 수 있도록 규정함.

- 위의 개별 법률에서 이와 같이 규정한 것은 금융·신용정보라는 민감한 개인정보에 대하여 정보주체의 통제권과 자기결정권을 강화하고 정보의 오남용을 방지하는 데 그 취지가 있다고 할 것임.

- 그러나 개정안은 전기통신금융사기의 발생 및 피해 확산이 의심되는 상황에서 이를 적시에 신속하게 대응·차단하기 위하여 사기정보제공기관, 정보공유분석기관 및 사기정보이용기관이 수집한 정보를 정보주체의 동의 없이 공유·제공·활용할 수 있도록 하려는 것인바,

개정안의 입법 취지를 효과적으로 달성하기 위하여는 「금융실명거래 및 비밀보장에 관한 법률」 및 「신용정보의 이용 및 보호에 관한 법률」에 대한 특례를 부여하여 정보 제공 시 정보주체의 사전동의 생략 등을 허용할 필요성이 인정됨.

나타내는 증표를 내보이거나 전화, 인터넷 홈페이지의 이용 등 대통령령으로 정하는 방법으로 본인임을 확인받아 신용정보회사등이 가지고 있는 신용정보주체 본인에 관한 신용정보로서 대통령령으로 정하는 신용정보의 교부 또는 열람을 청구할 수 있다.

- 개정안은 정보보호 관련 개별법에 대한 특례를 규정하고 있어 개인정보 자기결정권이 일부 제한되는 측면이 있으나, 안 제13조의4제7항에서 취득한 정보를 목적 범위 내로 사용하도록 하고 정보주체가 해당 정보 또는 정보 제공사실을 조회할 수 있도록 사후적 안전관리 조치를 규정하고 있다는 점을 종합적으로 고려할 필요가 있을 것임.
- 따라서 개정내용의 입법 여부는 전기통신금융사기 예방·차단을 통한 정보주체의 재산권 등 보호의 필요성과 정보주체의 개인정보 자기결정권(사전통제권) 간의 법익 비교형량을 토대로 입법 정책적으로 결정할 필요가 있다고 보임.

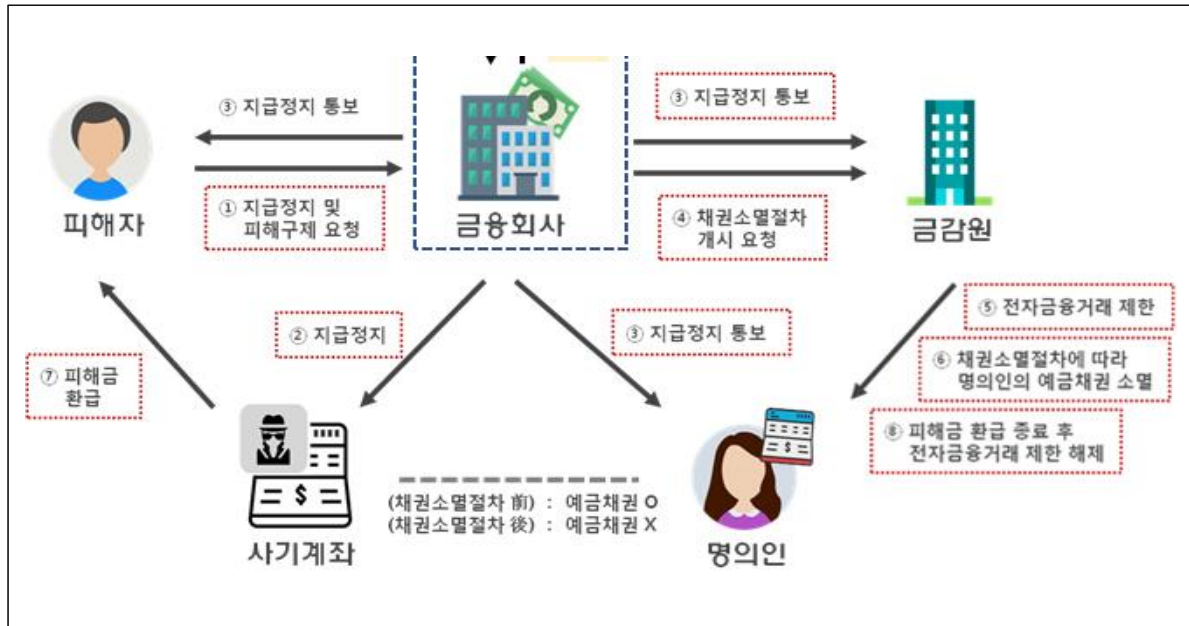
□ 제정 목적

- 전기통신금융사기(보이스피싱) 방지 및 피해금 환급 절차 등을 정하여 피해를 예방하고 재산상 피해를 신속 회복('11년 제정)

□ 주요 내용

- **(정의)** “전기통신금융사기”란 전기통신을 이용하여 타인을 기망·공갈하여 재산상의 이익을 취하거나 제3자가 취하게 하는 행위*
 - * 송금·이체하도록 하는 행위, 개인정보를 알아내어 송금·이체하는 행위, 자금을 교부받거나 교부하도록 하는 행위, 자금을 출금하거나 출금하도록 하는 행위
 - 재화의 공급·용역의 제공 등을 가장한 행위는 제외하되, 대출의 제공·알선·중개를 가장한 행위는 포함
- **(임시조치)** 금융회사 자체점검으로 의심거래계좌라고 추정되면 계좌의 전부·일부의 이체·송금을 지연시키거나 일시정지 등 조치
- **(거래목적 확인)** 금융회사는 계좌 개설, 이체·출금 한도 제한시 고객의 금융거래의 목적을 확인하고 관련 업무지침 운영
- **(지급정지)** 금융회사는 ①피해자 신고, ②자체점검, ③수사기관의 요청시 즉시 해당 계좌의 전부에 대하여 지급정지 조치
- **(피해금 환급)** 금융회사는 지급정지 즉시 금융감독원에 명의인의 채권이 소멸되는 절차 개시를 요청하고
 - 기간(2달) 경과 후 환급 받을 자 및 그 금액을 결정하여 금융회사에 통지하면 금융회사는 지체없이 피해자에게 환급
- **(주요 벌칙)** 전기통신금융사기를 행한 자는 1년 이상의 유기징역 또는 범죄수익의 3배 이상 5배 이하에 상당하는 벌금, 허위 신청자는 3년 이하의 징역 또는 3천만원 이하의 벌금 부과

<보이스피싱 피해구제 절차 >



절차	내용	법 조항
① 지급정지 및 피해구제 요청	보이스피싱 피해자가 사기범에게 자금을 이체한 계좌(사기계좌)에 대한 지급정지(입출금·이체 금지) 요청 및 피해구제 신청	§3①
② 지급정지	금융회사가 보이스피싱 사기이용계좌에 대한 지급정지 실시(입출금·이체 금지)	§4①
②-① 정보공유	금융회사는 선불업자를 통해 공유된 사기이용계좌에 대해서도 지급정지 실시	§15③
③ 지급정지 통보	금융회사가 금감원, 명의인, 피해자 등에게 지급정지 사실을 통보	§4②
④ 채권소멸절차 개시 요청	금융회사가 금감원에 사기이용계좌 명의인의 예금채권을 소멸하기 위한 절차 개시 공고 요청	§5①
⑤ 전자금융거래 제한	금감원이 ③에 따라 통보받은 명의인을 전자금융거래 제한 대상으로 지정	§13의2
⑥ 채권소멸절차	④의 요청에 따라, 금감원이 채권소멸절차가 개시된 사실을 공고 (이의제기 등 없을시) 2개월 후 예금채권 소멸	§5② §9①
⑦ 피해금 환급	채권소멸 후 금감원이 14일 내 피해환급금을 산정하여 피해금 환급 결정 → 금융회사를 통해 피해금 환급	§10①
⑧ 전자금융거래 제한 종료	피해금 환급 지급이 종료된 경우 전자금융거래 제한 종료	§8①

※ 임시조치 : 금융회사는 자체점검을 통해 파악된 피해의심거래계좌에 대하여 이체·출금을 지연시키거나 일시정지(법 §2조의5①) → 임시조치 후에는 지체없이 본인확인 후 지급정지 or 임시조치 해제

(자료: 금융위원회)

참고2

보이스피싱 AI 플랫폼(ASAP) 개요

1. 개요

□ 금융·통신·수사 분야의 보이스피싱 의심정보를 집중하고 AI 기술로 패턴 분석 등을 통해 피해가능성을 선제 파악·대응

○ (운영주체) 금융보안원 ※ 「이상거래정보 공유시스템(FISS)」 고도화

○ (참여기관) **주금융권·전자금융업자 <FISS 기참여> +**
통신3사(SKT, KT, LGU+) + 수사기관 <신규참여 필요>

※ 참여범위는 순차 확대(예 : 제1금융권 → 제2금융권 → 통신사)

2. 정보 공유·활용 방안

□ (집중) 금융사·통신사·수사기관 등이 자체 FDS 등으로 파악한 의심정보를 「AI 플랫폼」에 집중

□ (공유) 긴급공유 정보와 AI분석 정보로 구분하여 공유

○ (긴급공유 정보) 피해자 신속구제를 위해 즉시 공유가 필요한 정보*

* (예) 악성앱 노출자 피해정보, 보이스피싱에 활용된 것으로 확인된 계좌정보 등

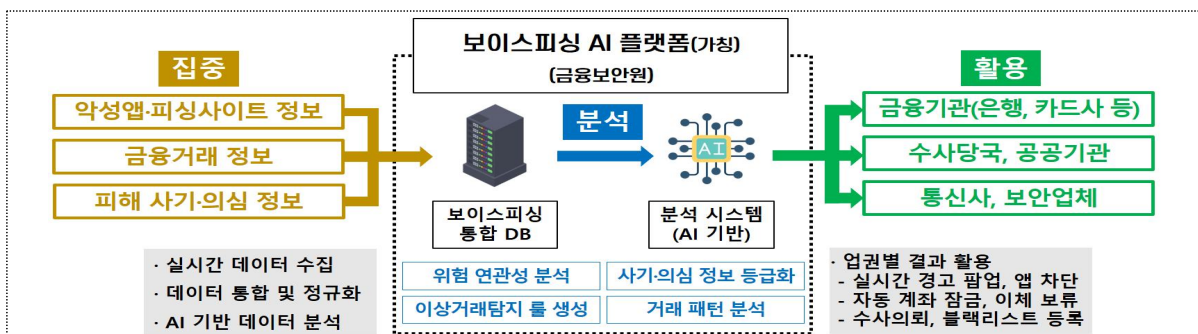
○ (AI분석 정보) 의심정보를 AI모델을 활용하여 분석한 결과 정보

□ (활용) 보이스피싱 사전차단·피해자 구제 등에 활용

○ (긴급공유 정보) ①이용자 경고, ②입출금 시도시 영상통화 등 문진 강화, ③이체된 자금에 대한 지급정지 등

○ (AI분석 정보) ①금융사, 통신사 등의 이상거래탐지 모델 고도화, ②취약 위험군(예 : 60대 이상, 소상공인) 집중 모니터링, ③ 수사 참고

< 보이스피싱 AI 플랫폼 체계도 >



(자료: 금융위원회)

참고3

금융보안원 개요

- 금융보안원은 금융권 침해위협 정보 수집·분석·공유, 침해사고 대응 등 보안 지원을 위해 '15.4월 설립된 비영리사단법인

* '14년 「카드 3사 개인정보 유출」 사건의 후속 조치로 금융보안 전담기구 설립 발표 ('14.3.10.)

- 전자금융거래법, 신용정보법 등에서 해당 기능을 부여*

* [전금법] 침해사고 대응 기관, [신정법] 정보보호 상시평가 수행기관, [정통망법·개보법] 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증기관

※ 금융보안원 일반 현황

- (조직·인력) 4본부(8부·3센터·3실), 311명('25.6월말 기준)
- (사원) 은행, 증권, 보험, 카드 등 총 207개 기관('25.10월 기준)
- (재원) 사원기관이 분담하는 회비로 운영('25년 예산 869억원)

- (기능) 금융보안 관련 예방, 평가·인증, 사고대응 등 기능 수행
 - (보이스피싱) 보이스피싱 정보를 금융회사 등에 실시간 공유하여 범죄 시도를 사전에 차단할 수 있도록 지원
 - (예방) 보안관제, 취약점 분석·평가, 모의해킹, 사이버위협정보 분석·공유, 금융보안 기술 연구 및 보급 등
 - (인증) 정보보호 상시평가 수행, 금융회사 정보보호관리체계 인증(ISMS, ISMS-P) 수행 등
 - (사고대응) 보안사고 발생시 현장조사 및 사고수습(복구 등) 지원 등

(자료: 금융위원회)

문 의 처
02)6788-5108