넥서스 리서치 2026_61 · NEXUS Research 2026_61 · NR-2026-061

오픈뱅킹은 모든 계좌가 아니라 연결한 권한을 연다

등록·조회·출금·안심차단·손해배상 규칙을 공식 원문으로 나눠 본다

오픈뱅킹 앱 하나를 쓰면 모든 계좌가 자동으로 열리는가. 금융결제원 설명은 다르다. 이용자는 앱에서 동의 절차를 거쳐 계좌를 등록하고, 앱은 그 계좌에 발급된 핀테크이용번호와 접근 토큰으로 허용된 기능을 호출한다.

그렇다고 위험이 작다는 뜻은 아니다. 2025년 10월 기준 고유 등록 계좌는 2억 5,800만 개다. 한 앱에 여러 계좌를 연결할수록 탈취된 인증·접근 수단이 닿는 범위는 넓어진다. 다만 공개된 피해 통계는 그 가운데 오픈뱅킹 경유분을 따로 보여 주지 않는다.

이 보고서는 '모두 열린다'는 공포와 '동의했으니 모두 사용자 책임'이라는 단정을 함께 걷어 낸다. 등록, 조회, 출금, 차단, 사고 책임을 서로 다른 규칙으로 읽는다.

발행일 2026년 8월 28일 **자료 기준일** 2026년 8월 28일 **분량** 본문 18쪽

넥서스 금융경영연구소
NEXUS Finance and Management Institute

SUMMARY

세 줄 요약

무엇을 물었나

오픈뱅킹에 계좌를 연결하면 무엇이 허용되는가. 의심거래가 생기거나 사고가 났을 때 무엇을 먼저 막고, 책임은 어떤 기준으로 나뉘는가.

무엇을 알아냈나

앱은 사용자가 등록하고 동의한 계좌에 한해 접근 토큰과 핀테크이용번호로 조회·이체 기능을 쓴다. 2025년 10월 고유 등록 계좌는 2억 5,800만 개였지만, 공개된 피해 통계는 오픈뱅킹 경유분을 따로 떼어 보여 주지 않는다. 안심차단은 신규 등록과 이미 등록된 계좌의 오픈뱅킹 조회·출금을 막지만 기존 연결을 자동 해지하지는 않는다.

읽는 사람은 무엇을 하면 되나

평소에는 어카운트인포의 '내 오픈뱅킹 한눈에'에서 쓰지 않는 연결을 해지한다. 추가 차단이 필요하면 오픈뱅킹 안심차단을 신청한다. 이미 의심 이체가 보이면 연결 해지보다 먼저 112에 신고하고 본인계좌 일괄지급정지를 요청한다.

이 보고서가 단정하지 않는 것

- 등록 계좌 수는 잔액이나 피해액이 아니다.
- 2021년 API 이용 비중은 그 달의 이용 구조이지 2026년 현재 비중이 아니다.
- 전체 보이스피싱 피해액을 오픈뱅킹 피해액으로 바꾸어 읽지 않는다.
- 전자금융거래법 제9조가 모든 사기 피해를 자동 배상한다고 말하지 않는다.

차례

1장

3,900만 명이 2억 5,800만 계좌를 연결했다

얼마나 많은 사람이 얼마나 많은 연결을 만들었는가.

금융위원회는 오픈뱅킹을 금융회사와 핀테크기업이 표준 방식으로 조회·이체 기능을 제공할 수 있게 만든 공동 금융 인프라라고 설명한다. 2019년 12월 전면 시행 뒤 6년이 지나면서 '한 앱에서 여러 계좌를 본다'는 행동은 별도 서비스가 아니라 일상의 금융 화면이 됐다.[1]

2억 5,800만 계좌

2025년 10월 고유 등록 계좌

고유 이용자 3,900만 명, 이용기관 138곳. 금융위원회가 2025년 11월 발표한 값이다.

오픈뱅킹 공개 규모의 두 시점

기준 시점	고유 이용자	고유 등록 계좌	이용기관
2021년 12월	3,000만 명	1억 계좌	120곳
2025년 10월	3,900만 명	2억 5,800만 계좌	138곳

자료: 금융위원회, 오픈뱅킹 시행 2주년 성과(2021.12.21); 오픈뱅킹 오프라인 서비스 개시(2025.11.18).

계좌 수가 이용자 수보다 훨씬 빠르게 늘었다

공개 수치만 단순 비교하면 이용자는 2021년 말 3,000만 명에서 2025년 10월 3,900만 명으로 30% 늘었다. 같은 기간 등록 계좌는 1억 개에서 2억 5,800만 개로 158% 늘었다. 이용자 한 명당 등록 계좌를 단순히 나누면 약 3.3개에서 약 6.6개가 된다. 이 계산은 개인별 실제 연결 수를 보여 주는 통계가 아니다. 다만 이용자 증가보다 계좌 연결의 밀도가 더 빠르게 높아졌다는 방향은 확인할 수 있다.

연결이 늘어난 이유를 피해 위험 하나로 설명할 수는 없다. 은행 계좌뿐 아니라 증권계좌, 선불충전금, 보험과 대출 정보까지 표준 API 범위가 넓어졌고, 2025년에는 은행 영업점에서도 다른 금융회사 계좌를 등록·조회할 수 있게 됐다. 편익이 넓어진 만큼 한 사람이 관리해야 할 연결도 많아졌다.

'등록 계좌'는 돈의 크기가 아니다

2억 5,800만이라는 숫자는 잔액도, 거래 건수도, 공격 가능한 계좌 수도 아니다. 금융위원회 발표가 밝힌 것은 중복을 제거한 등록 계좌 수다. 휴면 여부, 잔액, 출금이체 동의 여부, 앱별 권한 범위는 이 숫자에 함께 제시되지 않았다. 따라서 이 수치를 근거로 '2억 5,800만 계좌가 모두 즉시 출금 가능하다'고 읽으면 공개자료의 범위를 넘어선다.

반대로 숫자가 크다는 사실을 가볍게 볼 수도 없다. 연결 하나마다 사용자가 기억하고 관리해야 할 관계가 생긴다. 앱을 삭제했지만 연결은 남아 있을 수 있고, 한 계좌가 여러 서비스에 등록돼 있을 수도 있다. 오픈뱅킹의 생활 위험은 '전체 금융망이 한 번에 열린다'기보다 '오래전에 허용한 연결을 지금도 알고 있는가'에 가깝다.

확인된 것과 확인되지 않은 것

- **확인:** 2025년 10월 고유 등록 계좌 2억 5,800만 개, 고유 이용자 3,900만 명, 이용기관 138곳.
- **미확인:** 개인별 연결 분포, 출금동의가 살아 있는 계좌 비중, 장기 미사용 연결 비중.

이 장에서 확인할 것

등록 계좌 수를 잔액·피해액·출금 가능 계좌 수와 바꾸어 읽지 않는다.

확인 위치: 금융위원회 규모 발표의 지표 정의와 기준 시점.

[1] 금융위원회, 「오픈뱅킹 오프라인 서비스 개시」, 2025.11.18. 자료는 서비스 시작을 2019년 12월로 설명하고 2025년 10월 규모를 제시한다.

2장

앱은 모든 계좌가 아니라 등록한 계좌와 권한을 연다

'연결'이라는 한 단어 안에 어떤 절차와 기능이 들어 있는가.

금융결제원 개발자 문서는 사용자가 앱에서 오픈뱅킹 이용에 동의하면 앱이 접근 토큰을 발급받고, 등록 계좌별 핀테크이용번호를 사용해 API를 요청한다고 설명한다. 계좌를 등록하는 절차와 그 계좌에서 무엇을 할 수 있는지는 한 단계가 아니다.[2]

등록은 네 단계를 지난다

① 앱 신청

이용자는 금융회사나 핀테크 앱에서 오픈뱅킹 연결을 선택한다.

② 인증·동의

금융결제원 사용자 인증 화면에서 본인을 확인하고 계좌 접근 및 출금이체 관련 동의를 한다.

③ 토큰 발급

앱은 사용자 동의를 바탕으로 접근 토큰을 발급받는다. 토큰은 API 호출 때 권한을 증명하는 값이다.

④ 계좌별 번호

등록한 계좌에는 이용기관과 사용자의 조합에 고유한 핀테크이용번호가 부여된다. 앱은 이 번호와 토큰으로 등록 계좌 기능을 요청한다.

이 구조에서 '앱 하나가 뚫리면 모든 계좌가 열린다'는 문장은 두 가지를 섞는다. 첫째, 이용자의 모든 금융계좌가 자동으로 연결되는가. 공식 절차상 그렇지 않다. 둘째, 이미 여러 계좌를 한 앱에 등록해 둔 상태에서 인증정보나 토큰이 탈취되면 여러 연결 계좌가 함께 영향을 받을 수 있는가. 허용 범위와 보안 통제가 뚫렸다면 가능성이 생긴다. 위험의 단위는 '세상의 모든 계좌'가 아니라 '그 앱에 등록돼 있고 해당 기능이 허용된 계좌'다.

기능별로 다른 오픈뱅킹 권한

기능	무엇을 가져오거나 움직이나	사용되는 핵심 값	사용자가 확인할 것
계좌 목록	등록 가능한 본인 계좌 목록	사용자 인증·동의	어떤 계좌를 실제 등록했는가
잔액 조회	등록 계좌의 현재 잔액	접근 토큰, 핀테크이용번호	조회 권한이 필요한 앱인가
거래내역 조회	지정 기간 입출금 내역	접근 토큰, 핀테크이용번호	거래정보 노출 범위를 감수하는가
출금이체	등록 계좌에서 자금 출금	출금동의, 토큰, 계좌 식별값	출금동의를 했는가, 한도는 무엇인가
입금이체	수취 계좌로 자금 입금	토큰, 수취 계좌 정보	앱의 송금 기능을 실제 쓰는가

자료: 금융결제원 오픈뱅킹 API 명세와 OAuth 인증 안내. 표의 '확인할 것'은 연구소 정리.

동의는 법률상 출금의 출발점이다

전자금융거래법 시행령 제10조는 지급인이 출금에 동의하는 방법으로 서면, 전자서명된 전자문서, 전화 녹취 등을 둔다. 오픈뱅킹의 사용자 인증 화면은 단순 회원가입 화면이 아니라 계좌 접근과 출금 지시의 법적·기술적 출발점이 된다. 그래서 동의 화면을 통과했다는 사실만 확인할 것이 아니라 무엇에 동의했는지를 나눠 보아야 한다.

계좌를 조회하는 권한과 돈을 출금하는 권한은 결과가 다르다. 거래내역 조회는 자금을 움직이지 않지만 소비 패턴과 급여, 거래 상대방을 드러낸다. 출금이체는 자금을 실제로 움직인다. 두 권한 모두 침해될 경우 손해가 생길 수 있으나 손해의 종류와 긴급 대응은 다르다.

앱 삭제와 연결 해지는 같은 동작이 아니다

휴대전화에서 앱을 지우는 것은 단말기에서 프로그램을 삭제하는 일이다. 오픈뱅킹 계좌 등록 관계를 없애는 일은 금융결제원 계좌정보통합관리서비스나 해당 앱에서 별도로 해야 한다. 금융결제원은 계좌 해지 API도 별도로 제공한다. 따라서 '더 이상 안 쓰는 앱'의 위험을 줄이려면 아이콘 삭제가 아니라 연결 목록 확인과 해지가 필요하다.

권한을 점검할 때 묻는 세 질문

1. 이 앱에 지금도 연결된 계좌가 무엇인가.
2. 잔액·거래내역 조회만 필요한가, 출금이체까지 필요한가.
3. 앱을 쓰지 않게 됐을 때 연결도 해지했는가.

이 장에서 확인할 것

앱 설치, 사용자 동의, 계좌 등록, API 권한을 하나의 행위로 묶지 않는다.

확인 위치: 금융결제원 사용자인증 화면과 해당 앱의 연결 계좌 목록.

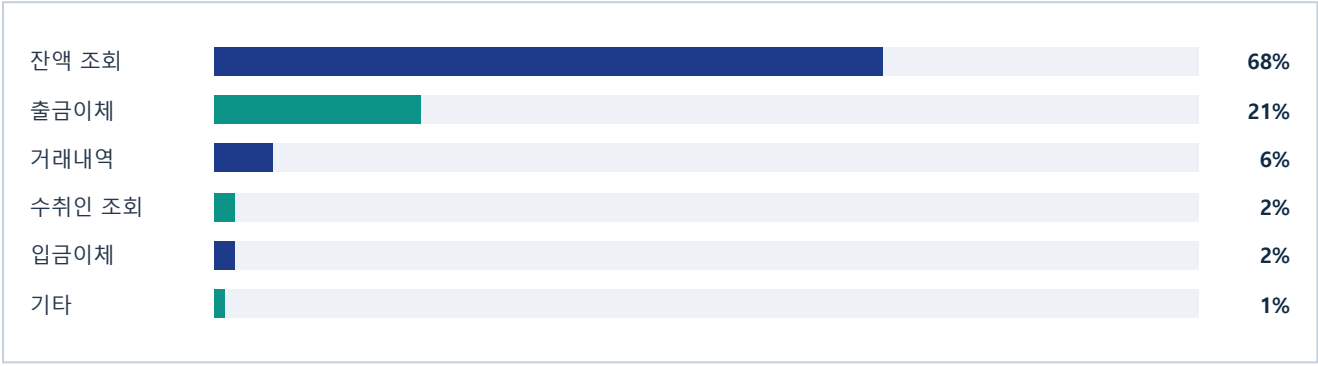
[2] 금융결제원, 오픈뱅킹 개발자사이트「사용자인증」및「OAuth 2.0」. 핀테크이용번호는 이용기관과 사용자 조합에서 등록 계좌를 식별하는 번호다.

3장

조회가 68%, 출금이체가 21%였다

사람들이 실제로 많이 쓴 기능과 위험이 생기는 기능은 같은가.

금융위원회가 공개한 2021년 11월 API 이용 구성에서 잔액 조회가 68%로 가장 컸고 출금이체가 21%로 뒤를 이었다. 거래내역 조회 6%, 수취인 조회 2%, 입금이체 2%, 기타 1%였다. 오픈뱅킹의 일상 기능은 '한 화면에서 보는 것'이 중심이지만 자금을 움직이는 호출도 다섯 건 가운데 한 건꼴이었다.[3]



자료: 금융위원회, 「오픈뱅킹 시행 2주년 및 오픈파이낸스 발전방안」, 2021.12.21. 기준: 2021년 11월.

조회 위험과 이체 위험은 다르게 막아야 한다

잔액·거래내역 조회 권한이 침해되면 공격자는 계좌 잔액, 급여일, 반복 결제, 거래 상대방을 파악할 수 있다. 곧바로 돈이 빠져나가지 않더라도 더 정교한 사칭과 표적형 사기의 재료가 된다. 출금이체 권한 침해는 자금 이동으로 이어질 수 있어 시간의 중요성이 더 크다. 사용자는 '조회만 했으니 괜찮다'거나 '돈이 빠졌으니 오픈뱅킹 탓이다'라고 한 단계로 결론내리지 말고 어떤 기능이 호출됐는지 거래 기록으로 확인해야 한다.

한도가 있다고 위험이 사라지지는 않는다

금융위원회는 2022년 보이스피싱 예방 대책에서 비대면 계좌 개설 뒤 3일 동안 오픈뱅킹 이체를 제한하고, 다른 목적의 이용 한도를 하루 1,000만 원에서 300만 원으로 낮추는 방안을 제시했다. 이 자료는 당시 정책 설계를 보여 주지만, 모든 기관·모든 계좌에 2026년 현재 동일한 300만 원 한도가 적용된다는 근거로 쓸 수는 없다. 한도는 이용기관, 서비스, 본인확인 방식과 시행 규정에 따라 확인해야 한다.

한도는 최대 피해를 줄이는 장치이지 접근 자체를 무효로 만드는 장치가 아니다. 반복 거래, 여러 등록 계좌, 다른 이체 수단이 결합되면 단일 한도만으로 전체 노출을 설명할 수 없다. 그래서 보안 통제는 한도, 이상거래탐지, 추가 인증, 등록 차단, 지급정지를 겹쳐 둔다.

운영기관도 보안 통제를 강화해 왔다

금융위원회는 2021년 7월 오픈뱅킹 참여기관 보안 관리 방안을 강화했고, 같은 해 12월 이상거래탐지시스템 고도화를 추진했다고 밝혔다. 참여 전에 보안 적합성 점검을 거치고, 이용 중에도 거래 패턴을 탐지하는 구조다. 이 사실은 사고가 불가능하다는 뜻이 아니다. 오히려 다수 기관이 하나의 표준망을 쓰는 만큼 앱·기관·공동망·이용자 단말의 통제를 함께 살펴야 한다는 뜻이다.

조회 단계

정보 노출과 사칭 재료의 확산을 본다.

이체 단계

출금동의·토큰·추가 인증·한도·이상거래탐지를 본다.

사고 뒤

거래 시각·접속 기록·신고 시각·지급정지 여부를 보존한다.

이 장에서 확인할 것

2021년 기능별 이용 비중은 역사적 관측값으로만 쓰고 현재 비중으로 확대하지 않는다.

확인 위치: 금융위원회 2021년 12월 발표의 집계 월과 단위.

[3] 2021년 11월의 API 이용 비중이다. 당시 일평균 거래는 2,000만 건, 일평균 거래금액은 약 1조 원으로 발표됐다. 이 값 역시 당시 규모다.

4장

사고 책임은 한 문장으로 정해지지 않는다

앱, 금융회사, 이용자 가운데 누가 배상하는가.

전자금융거래법 제9조는 접근매체의 위조·변조, 계약 또는 거래지시의 전자적 전송·처리 과정에서 생긴 사고, 침입으로 획득한 접근매체 이용 사고 등으로 손해가 나면 금융회사 또는 전자금융업자가 배상할 책임을 진다고 정한다. 대법원도 이 조항을 법정 무과실책임으로 설명한 바 있다.[4]

그러나 '오픈뱅킹 사고'라는 말만으로 제9조가 곧바로 적용되지는 않는다. 실제로 어떤 접근매체가 쓰였는지, 정상 인증이었는지, 전송·처리 사고가 있었는지, 이용자가 사기범에게 직접 이체했는지, 침해된 주체가 누구인지가 갈린다. 같은 피해액이라도 거래 경로가 다르면 법적 평가가 달라질 수 있다.

사고 장면별 먼저 확인할 사실

장면	핵심 확인	제9조 판단의 쟁점
접근수단 위조·변조	누가 어떤 인증값을 만들거나 바꿨는가	법이 정한 사고 유형인지
전송·처리 오류	사용자 지시와 실제 처리 결과가 달랐는가	전자적 전송·처리 과정 사고인지
침입 후 접근수단 이용	서버·망·단말 침입과 토큰 탈취가 있었는가	부정 획득 접근매체가 사용됐는지
사용자 직접 송금	사기 설명에 속아 본인이 거래를 승인했는가	제9조의 전자금융사고와 같은 유형인지
앱·대행자 과실	전자금융보조자의 시스템·절차에 잘못이 있었는가	제11조에 따라 금융회사 등의 과실로 볼 수 있는지

'중대한 과실'도 아무 실수나 뜻하지 않는다

법은 금융회사 등이 이용자의 고의나 중대한 과실을 입증하고 미리 약정한 경우 책임의 전부 또는 일부를 이용자가 부담하게 할 수 있도록 한다. 시행령 제8조는 중대한 과실의 범위를 구체적으로 좁힌다. 접근매체를 빌려주거나 맡기거나 양도한 경우, 권한 없는 제3자가 사용할 수 있음을 알았거나 쉽게 알 수 있었는데 접근매체를 누설·노출·방치한 경우, 정당한 이유 없이 추가 보안조치를 거부한 경우 등이 대표적이다.

따라서 '신분증 사진을 휴대전화에 저장했다'거나 '악성 앱이 설치됐다'는 사실 하나만으로 언제나 중대한 과실이라고 단정할 수 없다. 그 정보가 법상 접근매체인지, 제3자 사용 가능성을 쉽게 알 수 있었는지, 금융회사가 요구한 추가 보안조치를 거부했는지 등 시행령 요건과 구체적 경위를 보아야 한다. 반대로 비밀번호·인증서를 타인에게 넘겨준 사실이 확인되면 이용자 책임 판단에 중요하게 작용할 수 있다.

앱 운영자도 책임 구조 안에 있다

전자금융거래법 제11조는 전자금융보조자의 고의나 과실을 금융회사 또는 전자금융업자의 고의나 과실로 본다. 이용자에 대한 배상 책임과 사업자들 사이의 구상 관계를 분리하는 구조다. 이용자가 사고 직후 어느 회사가 최종 부담자인지 스스로 확정하지 못하더라도, 연결 앱과 출금 계좌 금융회사 양쪽에 사고 접수와 기록 보존을 요구할 이유가 여기 있다.

사고 뒤 책임을 가르는 기록

- 거래 일시, 금액, 수취계좌, 거래 구분
- 오픈뱅킹 계좌 등록·해지·동의 이력
- 로그인·기기 등록·추가 인증 알림
- 금융회사·앱·112에 신고한 정확한 시각
- 악성 앱 설치 여부와 원격제어 흔적

이 장에서 확인할 것

사고 이름보다 거래지시·인증·전송·처리 기록을 먼저 확보한다.

확인 위치: 출금 금융회사와 연결 앱의 사고 접수번호 및 기록 보존 요청.

[4] 전자금융거래법 제9조·제11조, 같은 법 시행령 제8조. 대법원 2014.1.29. 선고 2013다86489 판결은 제9조 책임의 성격과 사고 유형을 설명한다. 개별 사건에는 공표·시행 시점의 현행 법령과 사실관계가 적용된다.

5장

피해액은 크지만 오픈뱅킹 몫은 공개되지 않는다

전체 사기 피해와 오픈뱅킹 위험을 어디까지 연결할 수 있는가.

금융위원회는 2025년 1월부터 11월까지 보이스피싱 피해가 2만 1,588건, 1조 1,330억 원이라고 발표했다. 전년 같은 기간 1만 8,676건, 7,257억 원보다 건수와 금액이 모두 늘었다. 피해 규모가 크다는 사실은 분명하다.[5]

21,588건
2025년 1~11월 보이스피싱 피해 건수

1조 1,330억 원
같은 기간 피해 금액

분리 통계 없음
검토한 공개자료에서 오픈뱅킹 경유 피해의 별도 연속 통계

그러나 이 전체 피해액을 오픈뱅킹 피해액이라고 부를 수는 없다. 보이스피싱에는 사용자가 직접 송금한 경우, 카드·대출·대면 인출, 원격제어 앱, 명의도용 계좌, 오픈뱅킹을 포함한 여러 경로가 섞인다. 오픈뱅킹이 범행에 쓰였다는 사례가 있더라도 전체 통계에서 그 비중과 피해액을 계산하려면 경로별 분류가 필요하다.

공개자료로 알 수 있는 것과 없는 것

항목	공개 여부	해석 한계
오픈뱅킹 등록 규모	고유 이용자·계좌·기관 수 공개	출금동의·장기 미사용 연결 비중은 미제시
역사적 API 사용 구성	2021년 11월 비중 공개	2026년 현재 구성으로 볼 수 없음
전체 보이스피싱 피해	기간별 건수·금액 공개	오픈뱅킹 원인·경유분이 분리되지 않음
오픈뱅킹 안심차단	기능·신청·해제 방식 공개	차단 뒤 실제 피해 감소 효과는 아직 장기 통계 부족
사고 배상	법률상 책임 규칙 공개	오픈뱅킹 사고의 유형별 배상률·평균 처리기간 미제시

통계가 비어 있으면 인과관계도 비어 있다

등록 계좌가 늘어난 시기와 보이스피싱 피해가 늘어난 시기가 겹친다고 해서 앞의 변화가 뒤의 원인이라고 결론낼 수 없다. 같은 기간 사칭 수법, 원격제어, 대포통장, 가상자산, 범죄 조직의 운영 방식도 달라졌다. 오픈뱅킹 고유 위험을 측정하려면 최소한 사고가 발생한 앱, 사용된 API, 등록·동의 시점, 인증 수단, 피해액, 지급정지 시각을 익명화해 분리해야 한다.

이 공백은 이용자 행동에도 영향을 준다. 위험 크기를 정확히 알 수 없으면 모든 연결을 끊거나 아무 조치도 하지 않는 양극단으로 움직이기 쉽다. 현재 공개된 근거가 지지하는 중간 해법은 '쓰지 않는 연결은 해지하고, 신규 연결 자체를 막고 싶으면 안심차단을 쓰며, 사고가 의심되면 지급정지를 먼저 하는 것'이다.

안심차단은 2025년 11월에 시작됐다

금융위원회는 2025년 11월 14일부터 오픈뱅킹 안심차단 서비스를 시행했다. 이용자가 선택한 금융회사에 대해 신규 오픈뱅킹 등록을 막고, 이미 등록된 계좌의 오픈뱅킹 조회·출금 거래도 차단한다. 지역 농·축협 등을 포함해 3,608개 금융회사가 참여한다고 발표했다. 이 제도는 '연결을 이용한 거래'를 멈추는 사전 통제다.

다만 효과를 평가할 공개 시계열은 아직 짧다. 가입자 수, 차단 시도 건수, 차단으로 막힌 피해액, 오탐과 해제 불편을 함께 공개해야 제도의 실효성을 판단할 수 있다. 서비스가 있다는 사실과 피해를 얼마나 줄였는지는 다른 질문이다.

정책 공개가 더 필요한 네 숫자

1. 오픈뱅킹 경유 사고 건수와 피해액
2. 조회·출금·등록 탈취 등 사고 유형별 구성
3. 안심차단으로 거절된 신규 등록·거래 건수
4. 사고 접수부터 지급정지·환급·배상까지 걸린 기간

이 장에서 확인할 것

전체 보이스피싱 피해액과 오픈뱅킹 경유 피해액을 같은 숫자로 쓰지 않는다.

확인 위치: 금융위원회 피해 통계의 범죄 유형·거래 경로 분류.

[5] 금융위원회, 「보이스피싱 피해 현황 및 대응방안」, 2025년 1~11월 집계. 이 보고서는 해당 숫자를 오픈뱅킹 피해액으로 사용하지 않는다.

6장

연결 해지·안심차단·지급정지는 서로 다른 버튼이다

평소, 의심 단계, 피해 발생 뒤에 무엇을 해야 하는가.

계좌정보통합관리서비스의 설명에 따르면 오픈뱅킹 안심차단을 신청해도 기존 오픈뱅킹 등록 관계가 자동으로 삭제되지는 않는다. 연결을 끊으려면 '내 오픈뱅킹 한눈에 → 오픈뱅킹 조회·해지'에서 별도로 해지해야 한다. 차단과 해지는 함께 쓸 수 있지만 같은 기능이 아니다.[6]

세 조치의 목적과 한계

조치	언제	무엇을 막나	남는 것
연결 해지	평소 정리	선택한 앱·계좌의 등록 관계	다른 앱의 연결, 신규 등록 가능성
오픈뱅킹 안심차단	사전 예방·의심 단계	선택 금융회사의 신규 등록과 기존 등록 계좌의 오픈뱅킹 조회·출금	기존 등록 정보 자체, 오픈뱅킹 밖의 거래 수단
본인계좌 일괄지급정지	피해 의심·발생 직후	본인 명의 계좌의 출금·이체 등 자금 이동	사고 조사·피해구제 신청·접속기기 정리

평소: 연결 목록을 줄인다

어카운트인포 앱이나 계좌정보통합관리서비스에서 '내 오픈뱅킹 한눈에'를 연다. 현재 오픈뱅킹에 등록된 계좌와 이용기관을 확인하고 쓰지 않는 관계를 해지한다. 앱을 삭제한 지 오래됐거나 회사 이름을 알아보지 못한다면 우선 해지 대상이다. 해지 뒤 자주 쓰는 자동이체나 간편결제가 멈추지 않는지도 확인한다.

추가 차단: 신규 등록과 기존 거래를 묶어 막는다

오픈뱅킹 안심차단은 금융회사 영업점, 어카운트인포 앱, 은행 모바일 앱에서 신청할 수 있다. 금융회사별로 선택해 적용할 수 있다. 신청하면 해당 금융회사 계좌를 새로 오픈뱅킹에 등록할 수 없고 이미 등록된 계좌도 오픈뱅킹을 통한 조회와 출금이 제한된다.

불편도 있다. 금융위원회는 오픈뱅킹을 사용하는 간편결제, 지역화폐 구매 등이 제한될 수 있다고 안내한다. 해제는 비대면으로 할 수 없고 금융회사 영업점을 방문해야 한다. 보호 강도가 높은 대신 다시 쓰기 시작할 때 시간이 든다. 본인이 오픈뱅킹을 거의 쓰지 않거나 명의도용이 걱정될 때 적합하다.

피해 의심: 112와 지급정지를 먼저 한다

모르는 오픈뱅킹 등록 알림, 본인이 하지 않은 소액 인증 거래, 낯선 출금이 보이면 '어느 앱을 지울까'부터 고민하지 않는다. 112로 신고하고 본인계좌 일괄지급정지를 요청한다. 금융위원회가 안내한 통합신고 체계는 사건 접수, 악성 앱 차단, 계좌 지급정지와 피해구제 절차를 연계한다. 금융회사에도 사고를 접수해 거래 기록과 인증 기록 보존을 요청한다.

정상·정기 점검
어카운트인포에서 연결 목록 확인 → 불필요 연결 해지 → 출금동의와 알림 설정 점검.

명의도용 우려
오픈뱅킹 안심차단 신청 → 필요하면 비대면 계좌개설 안심차단·여신거래 안심차단도 함께 확인.
의심 이체 발견
112 신고와 본인계좌 일괄지급정지 → 금융회사·앱 사고 접수 → 기기·인증수단 점검 → 피해구제 신청.

‘안심차단을 했으니 연결도 없어졌다’고 생각하지 않는다

계좌정보통합관리서비스 FAQ는 안심차단이 기존 오픈뱅킹 등록 관계를 자동 삭제하지 않는다고 명시한다. 차단을 풀면 기존 연결이 다시 영향을 줄 수 있으므로, 장기적으로 쓰지 않을 앱은 차단과 별개로 해지한다. 반대로 연결을 해지했다고 신규 명의도용 등록이 막히는 것은 아니므로 그 우려가 크면 안심차단을 추가한다.

5분 점검표

- 모르는 이용기관이나 오래된 앱 연결이 없는가.
- 출금이체를 쓰지 않는 앱에 출금 권한이 남아 있지 않은가.
- 오픈뱅킹 등록·이체 알림을 받을 휴대전화 번호가 최신인가.
- 사고 때 바로 찾을 112와 주거래 금융회사 연락 경로를 저장했는가.
- 안심차단 해제는 영업점 방문만 가능하다는 점을 알고 있는가.

이 장에서 확인할 것

연결 해지, 안심차단, 지급정지 가운데 현재 상태에 맞는 조치를 고른다.

확인 위치: 어카운트인포 연결 목록, 안심차단 등록 현황, 112 신고 접수 내역.

[6] 금융결제원 계좌정보통합관리서비스 FAQ와 금융위원회「오픈뱅킹 안심차단 서비스 시행」, 2025.11.13. FAQ는 차단과 연결 해지를 별도 절차로 안내한다.

APPENDIX A

부록 가 · 용어 풀이

오픈뱅킹

금융회사와 핀테크기업이 표준 API로 조회·이체 등 금융 기능을 제공하도록 만든 공동 인프라.

API

서로 다른 프로그램이 정해진 형식으로 기능이나 데이터를 요청하고 돌려받는 접점.

접근 토큰

앱이 사용자 동의를 바탕으로 API를 호출할 권한이 있음을 증명하는 값.

핀테크이용번호

이용기관과 사용자 조합에서 등록 계좌를 식별하는 고유 번호.

출금이체

지급인의 동의를 받아 지급 계좌에서 자금을 출금하는 전자지급 방식.

접근매체

전자금융거래에서 거래지시를 하거나 이용자와 거래내용의 진실성·정확성을 확보하는 수단. 법률상 범위가 정해져 있다.

전자금융보조자

금융회사나 전자금융업자를 위해 전자금융업무 일부를 수행하는 자. 법은 이들의 고의·과실을 금융회사 등의 고의·과실로 본다.

일괄지급정지

피해 우려 때 본인 명의 계좌의 자금 이동을 한꺼번에 멈추도록 요청하는 조치.

APPENDIX B

부록 나 · 자료 출처와 각주

제도·수치·법률 문장은 1차 자료를 우선했다. '공개되지 않았다'는 문장은 아래 공개자료를 대조한 범위에 한정한다.

자료 출처

1. [1차] 금융위원회, 「은행권 오픈뱅킹 시범서비스 실시」, 2019.10.29. 확인 2026.08.28. fsc.go.kr/no010101/73746
2. [1차] 금융위원회, 「오픈뱅킹 시행 2주년 및 오픈파이낸스 발전방안」, 2021.12.21. 확인 2026.08.28. fsc.go.kr/no010101/77097
3. [1차] 금융위원회, 「오픈뱅킹 오프라인 서비스 개시」, 2025.11.18. 확인 2026.08.28. fsc.go.kr/no010101/85688
4. [1차] 금융위원회, 「오픈뱅킹 안심차단 서비스 시행」, 2025.11.13. 확인 2026.08.28. fsc.go.kr/no010101/85644
5. [1차] 금융결제원, 오픈뱅킹 서비스 개요, 발행일 미표기. 확인 2026.08.28. openapi.kftc.or.kr/service/openBanking
6. [1차] 금융결제원, 오픈뱅킹 사용자인증, 발행일 미표기. 확인 2026.08.28. openapi.kftc.or.kr/openapi/openbanking/userAuth
7. [1차] 금융결제원 개발자사이트, OAuth 2.0과 계좌 등록, 발행일 미표기. 확인 2026.08.28. developers.kftc.or.kr/dev/openapi/open-banking/oauth
8. [1차] 금융결제원, 잔액조회·거래내역조회 API 명세, 발행일 미표기. 확인 2026.08.28. 잔액조회, 거래내역조회
9. [1차] 계좌정보통합관리서비스, 오픈뱅킹 안심차단 FAQ, 발행일 미표기. 확인 2026.08.28. payinfo.or.kr/cs/faq/qryListWebFaq.do
10. [1차] 국가법령정보센터, 전자금융거래법 제9조·제10조·제11조 및 시행령 제8조·제10조, 현행 법령. 확인 2026.08.28. 전자금융거래법, 시행령
11. [1차] 대법원 2014.1.29. 선고 2013다86489 판결. 확인 2026.08.28. 국가법령정보센터 판례
12. [1차] 금융위원회, 「보이스피싱 피해 현황 및 대응방안」, 2025년 1~11월 집계, 2026.01.08. 확인 2026.08.28. fsc.go.kr/po010101/85959
13. [1차] 금융위원회, 「보이스피싱 원스톱 통합신고·대응센터」 안내, 2023.09.26. 확인 2026.08.28. fsc.go.kr/po010101/80830
14. [파생] 연구소 계산. 등록 계좌 증가율 = (2억 5,800만−1억)÷1억×100 = 158%. 이용자당 등록 계좌 근삿값 = 등록 계좌÷고유 이용자 = 2021년 약 3.3개, 2025년 약 6.6개. 계산·확인 2026.08.28.

각주

> 본문의 각주 1~6은 이 목록의 기관 원문을 장별로 묶어 표시한 것이다. 링크가 개정되거나 내용이 갱신될 수 있으므로 개별 사고 판단에는 확인일 이후의 현행 법령과 해당 금융회사의 거래 기록을 함께 확인해야 한다.

넥서스 금융경영연구소
NEXUS Finance and Management Institute

제목	오픈뱅킹은 모든 계좌가 아니라 연결한 권한을 연다
시리즈	넥서스 리서치 2026_61 · NEXUS Research 2026_61
발행	넥서스 금융경영연구소 · 2026년 8월 28일
자료 기준일	2026년 8월 28일
인용 형식	넥서스 금융경영연구소, 「오픈뱅킹은 모든 계좌가 아니라 연결한 권한을 연다」, 넥서스 리서치 2026_61, 2026.
수정 이력	없음
누리집	nexusfmi.com