

## NEWSLETTER

April 2024

법무법인(유) 광장 - 고려대학교  
침해사고 공동대응센터

Joint Incident Response Center

## CONTACT

공동센터장  
변호사 박광배T: 02,772,4343  
E: [kwangbae.park@leeko.com](mailto:kwangbae.park@leeko.com)공동센터장/  
고려대 정보보호대학원 교수  
김승주T: 02,3290,4897  
E: [skim71@korea.ac.kr](mailto:skim71@korea.ac.kr)

변호사 고훈경

T: 02,2191,3057  
E: [hwankyong.ko@leeko.com](mailto:hwankyong.ko@leeko.com)

변호사 차현정

T: 02,772,5971  
E: [hyunjeong.cha@leeko.com](mailto:hyunjeong.cha@leeko.com)비대면 휴대전화 개통 및 계좌 개설을 악용한 명의도용  
금융사기 관련 유의사항

최근 비대면으로 휴대전화 개통이 가능하다는 점을 악용하여 타인 명의의 휴대전화와 금융 계좌를 개설한 후 오픈뱅킹을 통해 자금을 가로채는 '명의도용 금융사기'가 문제되고 있기에, 본 뉴스레터에서는 이러한 명의도용 금융사기와 관련하여 유의할 사항들에 대해 소개하여 드리고자 합니다.

## I. 문제의 인식

비대면으로 알뜰폰 등 휴대전화를 개통할 때 이름과 주민등록번호를 통한 실명 확인(1단계 인증) 후 본인 인증(2단계 인증) 과정을 거치게 됩니다. 그런데, 최근 들어 기승을 부리는 크리덴셜 스테핑이나 스미싱 등을 통해 유출된 개인정보와 위조 또는 도용된 신분증을 활용하는 비교적 간단한 해킹을 통해 2단계 인증 절차를 우회하고, 이렇게 개통된 타인 명의의 휴대전화로 비대면 계좌를 개설한 뒤 오픈뱅킹을 통해 자산을 탈취하는 금융사기가 횡행하고 있습니다.

규제의 빈 틈을 노린 명의도용 금융사기의 수법은 날로 교묘해지고 있어 금융업계, 통신업계 뿐만 아니라 이용자 모두가 이러한 위험에 주목하고, 이에 대한 유의사항에 관심을 가질 필요가 있습니다.

## II. 비대면 방식의 휴대전화 개통 관련 유의사항

우선 휴대폰 개통의 경우, 한국정보통신진흥협회(KAIT)가 제공하는 '명의도용방지서비스' (Msafer)를 이용하면 본인도 모르게 휴대전화가 가입되는 것을 제한할 수 있습니다. 명의도용 방지서비스(Msafer)란 통신서비스 신규 개통시 가입사실을 명의자에게 통보하고 자신의 명의로 통신서비스에 가입된 현황을 한 곳에서 일괄 조회할 수 있게 해 명의도용을 방지하는 서비스입니다. 여기에는 가입사실 현황조사 서비스, 본인이 모르는 사이에 신규 휴대폰이 개통되는 것을 제한하는 가입제한 서비스, 휴대폰 개통이 이루어질 때 SMS/이메일로 통지해주는 서비스 설정 등이 있습니다.

이와는 별개로, 알뜰폰 개통 사이트 내 본인 인증 시스템에서 보안 문제가 불거지자 최근 과학기술정보통신부는 이동통신사와 알뜰폰 업계에 대책 마련을 주문했고, 이에 따라 대표적인 알뜰폰 사업자인 우정사업본부는 오프라인 창구에서 신분증 스캔을 도입하였고 인터넷우체국을 통한 알뜰폰 개통업무를 잠정 중단하는 등의 조치가 이루어진 것으로 보입니다. 향후 온라인에서의 알뜰폰 개통 절차가 강화될 것으로 예상되므로, 이러한 노력으로 최근의 금융사기 우려를 해소할 수 있을 지를 주시할 필요가 있을 것입니다.

### III. 비대면 방식의 계좌 개설 관련 유의사항

한편 금융회사에서 계좌 개설 시에는 금융실명거래 및 비밀보장에 관한 법률에 따른 실지명의를 확인하여야 합니다. 구체적으로 실명확인을 할 때 실명확인증표 사본(예: 주민등록증, 운전면허증, 여권 또는 외국인등록증의 사본) 제출, 영상통화 등 5가지 방법 중 2가지 이상의 방법을 의무적으로 적용하여야 합니다. 이중 영상통화 방법과 관련하여 최근 금융당국은 실시간 원격 얼굴인식 기술 등을 활용하여 비대면 방식으로 계좌 개설을 요청하는 사람이 계좌 개설을 요청하는 시점에 실제로 그 얼굴 등을 촬영하여 그 영상을 제출하는 것인지 여부를 확인하는 등 안면인식 시스템을 활용하도록 권장하고 있습니다.

한편, 비대면 계좌 개설과 관련하여서는 위 '명의도용방지서비스'(Msafar)와 유사하게 전체 금융회사의 비대면 계좌 개설을 일괄 제한할 수 있는 서비스는 제공되고 있지 않은 것으로 보입니다. 다만, 개별 금융회사에 따라서는 사전에 신청한 고객에 한하여 전자금융 로그인 제한 또는 비대면 오픈뱅킹 거래 제한 등의 서비스를 제공하고 있거나, AI 기반 신분증 원본 검증 시스템이나 영상통화를 이용한 이상거래 모니터링 시스템 구축 등 명의도용 금융사기를 방지하기 위한 다양한 노력도 기울이고 있는 것으로 보입니다.

그 이외에 금융감독원은 명의도용 금융거래사고를 예방하기 위하여 '개인정보 노출자 사고예방 시스템'을 운영하고 있습니다. 개인정보 노출사실을 등록하는 경우 등록된 개인정보는 금융회사에 공유되어 노출자 명의의 거래가 시도될 경우 신규계좌 개설, 신용카드 발급, 휴대전화 단말기 할부구입시 보증보험 가입, 오픈뱅킹 등 일부 금융거래를 제한시킬 수 있으며, 이렇게 제한된 금융거래를 재개하고자 하는 경우에는 등록 해제를 신청할 수 있도록 하고 있습니다.

그리고 2024년 4월 17일 금융위원회 정례회의에서 신용정보업감독규정 일부개정규정안을 의결하였는데, 이에 따라 올해 상반기에 금융거래 안심차단 서비스가 시행되면 소비자가 정보 유출, 명의도용, 보이스피싱 등으로 자신도 모르게 발생하는 신규 여신거래 등을 사전에 모두 차단할 수 있게 될 것으로 보입니다. 다만 위 서비스는 비대면 방식의 계좌 개설을 제한하는 것은 아니고 신규 여신거래를 사전에 차단하는 것입니다.

### IV. 시사점 및 향후 대응 방안

이처럼 비대면 방식으로 휴대전화 개통 또는 계좌 개설이 가능하다는 점을 악용한 명의도용 금융사기를 방지하기 위하여, 금융위원회와 금융감독원, 금융결제원과 금융보안원, 개별 금융회사까지 금융관련업계가 모두 관련 규제나 제도, 시스템을 개선하고 있으며, 과학기술정보통신부 및 이동통신 업계에서도 대책을 강구하고 있습니다. 그러나 이러한 규제나 제도, 시스템의 개선 속도에 앞서 명의도용 금융사기 방법이 진화할 가능성을 배제하기 어려운 것이 현실입니다. 또한 개별 금융회사 또는 이동통신사 취약점이 모두 다르기 때문에 별로 보안상 강점과 실제로 개선이 필요한 부분도 다르고 금융사고가 발생한 경우의 대응 방법도 다양할 수밖에 없을 것입니다.

따라서 금융, 통신 분야 뿐만 아니라 다양한 영역의 사업자들도 최근 금융사고의 변화 양상과 관련 규제의 변화에 촉각을 세우는 한편 개인정보의 유출, 도용을 통한 유사한 사고가 발생할 경우에 대비하여 법 위반이 문제될 수 있는 사항이 있을지를 사전에 검토하고, 필요한 경우 외부 전문가의 도움을 받아 회사의 잠재적 리스크에 대한 대응방안을 강구하시는 것이 바람직할 것입니다.

법무법인(유) 광장과 고려대학교 정보보호대학원은 갈수록 다양해지고 정교해지고 있는 금융사고/해킹 등 정보유출 사고의 예방 및 대응 지원이라는 목적하에 '침해사고공동대응센터'를 설립하고, 정보보호 법제와 기술의 유기적 결합을 통하여 제반 침해사고의 예방 및 대응을 위한 다양한 노력과 활동을 지원하고 있습니다. 이와 관련하여 궁금한 점이 있으시면 언제든지 법무법인(유) 광장 Data Privacy & Cybersecurity 그룹 또는 고려대학교 정보보호대학원으로 연락 주시기 바랍니다.

이 뉴스레터는 일반적인 정보 제공만을 목적으로 발행된 것으로서, 법무법인(유) 광장의 공식적인 견해나 법률의견이 아님을 알려드립니다. 법무법인(유) 광장에서 발송하는 뉴스레터를 원하지 않으시면 [수신거부](#)를 클릭해 주십시오.

[뉴스레터 더 보기](#)

**Lee  
& KO** 법무법인(유) 광장

서울 | 판교 | 북경 | 호치민시티 | 하노이  
02.772.4000 | [mail@leeko.com](mailto:mail@leeko.com) | [www.leeko.com](http://www.leeko.com)