

요약

딥페이크 금융사기는 안면인식을 우회하여 계좌를 개설하거나 임원을 사칭해 기업송금을 유도하는 등 수법이 고도화되고 있음. 이에 대응해 글로벌 금융권은 영상 합성 여부를 가려내는 데 그치지 않고, 영상이 실제 촬영기기에서 입력되었는지, 신분증이 발급기관 원본과 일치하는지, 송금 지시가 실제 권한자로부터 온 것인지를 독립된 수단으로 확인하는 등 검증체계를 강화하고 있음

○ 딥페이크 기술이 발달하면서 이를 이용한 금융사기도 빠르게 증가하고 있음

- 유럽 Citi Institute에 의하면 전체 사기 시도 중 딥페이크 비중은 2022년 0.10%에서 2024년 4.70%로 2년 만에 47배 증가하였으며¹⁾ 미국 저널 Journal of Accountancy는 2024년 글로벌 사기 시도 중 딥페이크 사기가 7%를 차지했다고 밝힘²⁾
- 합성한 얼굴로 안면인식을 우회하여 비대면으로 계좌를 개설하거나, 임원의 얼굴·음성을 조작해 기업송금을 유도한 사례가 확인되고 있음
 - 네덜란드에서는 타인의 신분증과 합성한 얼굴사진으로 네덜란드 3위 은행인 ABN AMRO의 비대면 실명확인을 우회해 2025년 3월부터 11월까지 약 8개월간 47개 계좌가 개설됨³⁾
 - 2024년 홍콩에서 직원이 최고재무책임자와 동료들이 등장하는 사전녹화 영상회의를 근거로 5개 계좌에 약 2억 홍콩달러를 이체한 사례가 발생함⁴⁾

○ 이에 대응해 글로벌 금융권은 영상 합성 여부를 가려내는 데 그치지 않고, 영상이 실제 촬영기기에서 입력되었는지, 신분증이 발급기관 원본과 일치하는지, 송금 지시가 실제 권한자로부터 온 것인지를 독립된 수단으로 확인하는 등 검증체계를 강화하고 있음

○ 영상 내용만 분석하는 방식은 실시간 딥페이크와 위조영상 삽입 공격에 취약할 수 있어, 실제 카메라에서 촬영됐는지 등 영상의 입력 경로까지 함께 확인할 필요가 있음

- 홍콩금융관리국(HKMA)은 2025년 8월 은행 앱이 단말기 카메라에 직접 접근해 영상을 수집하고, 무작위 생체 활성 검증(라이브니스)과 영상·배경 분석, 디지털 흔적 및 거래 모니터링, 수동심사를 연계하는 모범사례를 제시함
 - 이러한 영상의 입력 기기와 경로를 확인한 금융기관은 정교한 딥페이크 공격을 탐지하는 역량이 95% 이상 향상됨⁵⁾

1) Citi Institute(2025. 11.), "AI Deepfakes - When Seeing and Hearing Can't be Trusted"

2) Journal of Accountancy(2025. 5. 1.), "How CPAs can combat the rising threat of deepfake fraud"

3) Reichtbank Amsterdam(2026. 6. 17.), "2,5 jaar cel voor oplichten bank met deepfake-technologie"

4) The Government of Hong Kong(2024. 6. 26.), "LCQ9: Combating Frauds Involving Deepfake"

- 미국 국립표준기술연구소(NIST)는 비대면 본인인증 시 실제 촬영기기에서 입력되는지 확인하도록 요구하고, 이를 위해 가상 카메라, 가상 스마트폰, 스마트폰 탈옥·루팅⁵⁾ 등 영상 조작에 악용될 수 있는 환경을 탐지하도록 규정함⁷⁾
- 미국 금융범죄단속국(FinCEN) 역시 본인인증 중 은행 앱 대신 다른 웹캠 프로그램을 쓰거나 기술적 오류를 이유로 영상통화를 다른 수단으로 변경할 것을 요청하는 등 절차를 우회하려는 행태 자체를 의심거래 지표로 제시함⁸⁾

○ 한편 합성영상과 위조 신분증이 정교해져 제출된 영상·목소리를 판독하는 것만으로는 진위를 가릴 수 없게 되면서, 신분증과 통화 상대의 진위를 발급기관과 은행 앱으로 확인하는 방향으로 바뀌고 있음

- 홍콩은 공공 디지털 신원 플랫폼인 iAM Smart에 딥페이크 탐지와 NFC 기반 신분증 IC칩·이민국 기록 대조 기능을 도입하였으며, 금융당국은 이를 은행의 원격 계좌 개설에 적용하기 위한 시험을 2026년 중 시작할 계획임⁹⁾
- 호주 Commonwealth Bank는 고객이 은행과 통화할 때 은행 앱에 보안 메시지를 보내 실제 은행 직원과 연결되었는지를 확인하는 서비스를 운영함¹⁰⁾
- NIST 지침은 지문·얼굴 같은 생체정보만을 독립적인 인증수단으로 인정하지 않고, 휴대전화나 보안카드 같은 물리적 인증수단과 함께 사용하도록 규정하며 음성으로 인증하는 방식은 금지함¹¹⁾

○ 기존 방식은 직위나 긴급성을 내세운 지시를 그대로 승인함으로써 지시자의 사칭 여부나 결재 권한 보유 여부를 검증하지 못하였으므로, 관련 당국은 송금 지시가 전달된 경로와 다른 연락수단을 통해 지시자의 신원과 송금 권한을 다시 확인하도록 권고함

- 싱가포르 경찰·통화청·사이버보안청은 2025년 3월 공동권고문을 통해 임원이나 주요 이해관계자를 사칭한 통화·메시지의 진위 확인 절차를 마련하고, 갑작스러운 이체지시는 기존 연락경로를 통해 직접 확인하며, 자금이체 담당자를 우선 교육하도록 권고함¹²⁾

5) HKMA(2025. 8. 25.), "E-Banking Security ABCD"; HKMA(2025. 8. 25.), "Good Practices for Countering Deepfake Attacks"

6) 탈옥·루팅은 스마트폰 운영체제의 제한을 해제해 관리자 권한을 얻는 행위로, 카메라 영상 등의 데이터를 조작하는 데 악용될 수 있음

7) NIST(2025. 8.), "Digital Identity Guidelines: Identity Proofing and Enrollment (SP 800-63A-4)", §3.14

8) FinCEN(2024. 11. 13.), "Alert on Fraud Schemes Involving Deepfake Media", FIN-2024-Alert004

9) The Government of Hong Kong(2026. 6. 3.), "LCQ13: Measures to Tackle Identity Theft of Members of Public"

10) Commonwealth Bank of Australia(2023. 2.), "CallerCheck"

11) NIST(2025. 8.), "Digital Identity Guidelines – Authentication and Authenticator Management (SP 800-63B-4)", §3.2.3

12) Singapore Police Force, MAS and CSA(2025. 3. 12.), "Joint Advisory on Scams Involving Digital Manipulation"