

Korea's financial regulator calls emergency meeting over suspected AI-driven bank breaches

Source copy kept by wheresthe.ai for the story "Korea's financial regulator calls emergency meeting over suspected AI-driven bank breaches" (<https://wheresthe.ai/d/kr-bank-breaches-suspected-ai-attacks-2026-10/>).

Source: <https://www.koreajoongangdaily.com/business/from-banks-to-lenders-suspected-ai-hacks-expose-cracks-in-koreas-financial-defenses/12904281>

Text saved 18 Oct 2026 (the page as published).

SHA-256 of the saved text: fca709c94852082ad7dd3b4dc6fbb6151c203d2f1608d4d6d52705e7c9432d73

From banks to lenders, suspected AI hacks expose cracks in Korea's financial defenses

Breaches at banks, savings banks and consumer lenders exposed sensitive customer and loan data, raising fears of follow-on identity theft and fraud and spurring an emergency Financial Services Commission meeting.

News Team

News Team

Published October 4, 2026 - 6:49 p.m.

Modified October 4, 2026 - 8:07 p.m.

Make us preferred on Google

Financial Services Commission Chairman Lee Eog-weon, second from right, speaks during an emergency review meeting about recent data breaches on Oct. 4. NEWS1

A wave of suspected hacks using AI agents has spread from major commercial banks to smaller lenders, including savings banks and consumer finance companies. The breach exposed income and loan data, which has heightened concerns over follow-on crimes such as identity theft and impersonation fraud. "We cannot rule out the possibility that AI was used in the attacks," Financial Services Commission Chairman Lee Eog-weon said at an emergency meeting with financial industry representatives on Sunday. "The entire financial sector must recognize the gravity of the situation and remain on the highest alert."

Related Article

AI hackers target Korea's banks, trigger industrywide security review

State-run banks deny pressure to invest in controversial film 'Assassin(s)'

Korea signals deeper bond issuance cuts

Shinhan Bank data breach leaks personal, credit information of 25,000 customers

Authorities flagged weak authentication and excessive data retention and access as key weaknesses in the industry's defenses, and warned that similar security failures would face stern penalties. The Financial Supervisory Service alerted about 500 financial firms to malicious internet protocol, or IP, addresses identified across multiple attacks and issued security guidance. The firms must finish emergency checks and submit their findings by Thursday. An internal review at Welcome Savings Bank on Saturday uncovered a leak of up to 2,200 corporate customer records, which the bank reported to authorities. Compromised data included company names and the names, email addresses and phone numbers of handlers at affected companies. Yegaram Savings Bank had already disclosed a breach affecting about 40,000 customers on Friday after detecting signs of a leak on Wednesday. It is the largest breach disclosed so far at a single financial firm in the string of cyberattacks. Hyundai Capital also suffered a breach that exposed personal information belonging to some of its 146 mortgage loan agents. The latest cases show the attacks have spread beyond Korea's five major banks and into the secondary financial sector, which the Banking Act does not govern. Earlier breaches at major commercial banks — bound by the Banking Act — exposed the information of 25,727 customers at Shinhan Bank; 119 at KB Kookmin Bank; and 89 at Hana Bank. Personal information of 11 outsourced developers at BNK Busan Bank was also compromised.

A person stands in front of a row of ATMs from different banks. YONHAP

Even at Korea's largest banks, the attacks went undetected for hours and even days. Shinhan Bank took 15 hours and 26 minutes to detect its breach, Hana Bank took 41 hours and 44 minutes and KB Kookmin Bank needed 67 hours and 41 minutes. The delays have fueled concern that more breaches at other financial firms have yet to surface. Financial-sector breaches carry higher stakes than earlier leaks this year at telecom carrier SK Telecom, streaming service Tving and e-commerce platform Coupang last year. The data stolen in the latest bank breaches goes beyond names, contact details and resident registration numbers to borrowing records that can reveal a person's financial circumstances — such as customer identification numbers, loan application details, calculated credit limits, final decision codes and market interest rates. Stolen data can make voice-phishing scams far more convincing. A scammer could cite a victim's actual loan application, claim to be calling with the bank's decision and ask for additional verification or the installation of a malicious app. Because the caller already knows the victim's financial details, the approach could easily be mistaken for a legitimate call from the bank. Further, a password reset offers only limited protection once names, contact details, identification numbers and loan records have been exposed. Customers can ask their financial institution what information was compromised and use safeguards that block new credit transactions or remote account openings if needed. The industry argues that the data leaks should be separated from the security of banks' core transaction systems. The attacks targeted internet-facing systems used by employees and loan agents, not internal networks that manage account balances and transaction records.

A customer gets a loan consultation at a bank in Seoul on Sept. 14. NEWS1

Banks acknowledge that the external business systems targeted in the attacks may have had weaker security controls than core transaction systems. But they argue that the breaches don't amount to a compromise of the financial transaction system because the internal networks that manage customer balances and core transactions weren't breached. "Passwords and CVC numbers were not directly exposed, so the likelihood of immediate unauthorized transactions is low," a source from a financial regulatory agency said. Yet the hacking spree has rattled confidence in an industry regarded as one of the country's most secure. Customers are asking whether the money they put in banks is actually safe. Traces of a Chinese-language AI hacking tool called "Artex AI" were reportedly found in the attacks on major commercial banks. If increasingly sophisticated AI agents penetrate banks' internal networks, the threat could move beyond stolen personal data and strike at the accuracy and integrity of financial transactions.

BY KIM DA-YOUNG, OH HYO-JEONG [lee.soojung1@joongang.co.kr]

This article was originally written in Korean and translated by a bilingual reporter with the help of generative AI tools. It was then edited by a native English-speaking editor. All AI-assisted translations are reviewed and refined by our newsroom.

data breach business banking ai money industry fsc

Make us preferred on Google

Read more

Value of National Pension Service's stock holdings plunges as market tanks

The market value of the service's holdings fell 182 trillion won (\$136 billion) in three and a half months, with much of the investment concentrated in chipmakers.

Voice phishing fraud cases more than doubled in 2025, data shows

Fraud detection systems at five major banks flagged 1.11 million suspicious transactions as cybercrime concerns intensified.

AI boom to sustain Korea amid global headwinds for years, says senior IMF official

The IMF raised Korea's 2026 growth forecast to 3.3 percent as AI-driven semiconductor exports offset global economic risks.

Hyundai Motor to recall over 94,000 vehicles in U.S. over fire risk

The U.S. National Highway Traffic Safety Administration said that the front power seat motors may overheat if the power seat control switch is stuck, potentially causing a fire while the car is parked or driven.

See more articles

An Se-young reaches Denmark Open final, eyes ninth title of season

Value of National Pension Service's stock holdings plunges as market tanks

Korean won climbs to two-year high as chip exports boost dollar supply

KBO names 79 Golden Glove nominees as race for 10 awards begins

Voice phishing fraud cases more than doubled in 2025, data shows

Lee Kang-in, Hwang In-beom short-listed for AFC award as Son Heung-min misses cut

Number of inmates paroled before serving 60% of sentence rises

AI boom to sustain Korea amid global headwinds for years, says senior IMF official