FBI reportedly investigating second breach, this time involving the NCIC database



The FBI is reportedly investigating a cyberattack on the National Crime Information Center, a shared U.S. law enforcement database. The incident is unconfirmed and would be the bureau's second this year.

- Sources told CNN and the Associated Press that the attack on the NCIC occurred on a Thursday; the FBI did not comment.
- The NCIC is used by local, state and federal agencies to share data on criminals, fugitives, warrants and missing people.
- If confirmed, it is the FBI's second incident this year, after the ShinyHunters breach of its job site in September.
- Other U.S. agencies, including the ATF and the Departments of Defense, Transportation and

> Agriculture, also reported incidents this year.

The FBI is reportedly investigating a data breach involving the National Crime Information Center (NCIC), according to sources cited by CNN and the Associated Press. The attack is said to have happened on a Thursday. The FBI did not respond to requests for comment, so the incident remains unconfirmed.

What is known

The NCIC is a database that local, state and federal agencies in the United States use to share information on criminals and investigations. It includes data on outstanding warrants and other sensitive material that has value to criminals. The source does not describe how the attack happened, what data was accessed, or who is responsible.

President Donald Trump said he had been briefed and described the incident as not good. He added that the breach may give the public access to investigative files related to him.

Wider context

If confirmed, this would be the FBI's second incident this year. In September, the ShinyHunters group breached the FBI's job site and allegedly stole information on every FBI employee. Several people were arrested in that investigation.

Other U.S. government bodies have also been affected this year. A platform used by federal bankruptcy courts was taken down, and the ATF described an August ransomware attack as a major incident. The Departments of Defense and Transportation reported incidents, and the Department of Agriculture took payment systems offline after an attack last week.

Relevance for Saudi institutions

Nothing in the report points to exposure of Saudi organisations. It is nonetheless a useful reminder that shared databases used by many agencies concentrate risk, and that repeated incidents can affect even well-resourced bodies.

What to do now

1. Review which shared or multi-party databases your institution relies on and who has access to them.
2. Confirm that access to sensitive shared systems is limited by role and covered by strong authentication and logging.
3. Check that your incident response plan covers third-party and shared-platform compromises, including notification duties.
4. Monitor official sources for confirmed details before drawing conclusions or briefing leadership.