FBI Investigating Apparent Hack of National Criminal Justice Database



The FBI is reportedly investigating an apparent hack of the NCIC, its national criminal justice database. The scope is unclear and the bureau has declined to comment.

- A person familiar with the matter told AP the FBI is investigating an apparent hack of the National Crime Information Center (NCIC).
- The NCIC holds records on fugitives, missing persons, criminal history and stolen property, and is available to local, state and federal agencies.
- The scope of the problem was not immediately clear, and the FBI declined to comment.
- No immediate indication links the incident to recent government and private-sector outages, which officials attributed to routine upgrades and fixes.
- The FBI has been a frequent target, including a ShinyHunters data claim in September and an

> internal system investigation in March.

What is known

The FBI is investigating an apparent hack of the National Crime Information Center, known as the NCIC, according to a person familiar with the matter who spoke to The Associated Press on condition of anonymity. CNN reported it first. The FBI declined to comment, and the scope of the problem was not immediately clear.

The NCIC is a computerized database of criminal justice information shared with local, state and federal law enforcement agencies. It includes records on fugitives, missing persons, criminal history and stolen property.

Context

The news follows a series of digital outages in government and the private sector. Trump administration officials have said those were caused by routine upgrades and vulnerability fixes rather than a cyberattack. There is no immediate indication that the FBI incident is connected.

The bureau has been targeted before. In September, the ShinyHunters group said it had obtained a large trove of data on FBI employees and applicants and compromised the jobs portal. In March, the FBI disclosed it was investigating suspicious activity on an internal system holding sensitive surveillance and investigation information.

Why it matters for Saudi institutions

There is no stated Saudi impact. The incident is still a useful reminder for institutions that hold shared, sensitive records accessed by many parties: the exposure depends on how widely access is granted and how well it is monitored. Details are unconfirmed, so treat reporting as preliminary and avoid drawing conclusions about cause or impact until official information is available.

What to do now

1. Review which internal and external parties can access shared sensitive databases, and remove access that is no longer needed.
2. Confirm that logging and alerting cover queries and bulk exports on your most sensitive record systems.
3. Check that your incident response plan includes steps for an incident with unclear scope, including escalation and regulator notification.
4. Follow official updates rather than unconfirmed reporting before changing any controls or briefing the board.