

# OpenVoiceNews U.S.

Transparent. Unbiased. Yours.

## U.S. Judiciary Confirms Cyberattack on Court Records System

August 8, 2025

— Categories: Breaking News



The United States Federal Judiciary has confirmed that its electronic case management systems were targeted in a cyberattack, triggering swift action to strengthen the protection of sensitive court records. The incident highlights the increasing vulnerability of critical government systems to sophisticated and persistent cyber threats.

In an official statement, the Judiciary noted that while the majority of records in the Case Management/Electronic Case Files (CM/ECF) system are public, a smaller set of sealed filings contains highly sensitive or confidential information. These protected records now have stricter access controls in place to prevent unauthorized access and reduce the risk of further compromise. The agency described the cyberattack as both “sophisticated” and “persistent,” underscoring the seriousness of the breach.

“The federal Judiciary is taking additional steps to strengthen protections for sensitive case documents in response to recent escalated cyberattacks of a sophisticated and persistent nature on its case management system,” the statement read. It added that the agency is working closely with courts to mitigate any potential harm to litigants and to safeguard the integrity of legal proceedings.

The confirmation follows a *Politico* report earlier in the week that alleged the breach affected multiple federal judicial districts, disrupting both CM/ECF and the Public Access to Court Electronic Records (PACER) system. PACER is the primary platform that allows the public and legal professionals to access federal court filings. According to the report, the intrusion may have revealed sensitive details, including the identities of confidential informants. Anonymous sources claimed the Judiciary became fully aware of the breach’s scope on July 4, 2025, and subsequently held a related briefing without issuing an immediate public announcement.

Although the Judiciary stopped short of directly confirming that PACER’s confidential documents were accessed, its mention of working with courts to address the impact on litigants suggests that sensitive information may have been exposed. The agency has not disclosed the number of cases affected, the exact method of the breach, or the identity of the attackers.

The Judiciary also drew attention to the broader challenge of protecting older, legacy systems from increasingly advanced cyber threats. These vulnerabilities are not unique to the federal court system, as both public and private institutions face similar risks in defending critical infrastructure against targeted attacks.

BleepingComputer, a technology news outlet, reported that it sought further clarification from both the U.S. Federal Judiciary and the U.S. Department of Justice (DOJ). However, inquiries were met with referrals to the Judiciary’s published statement, leaving key questions about the incident unanswered.

The breach and the Judiciary’s subsequent response underscore the growing need for robust cybersecurity measures within essential government systems. While investigations are ongoing, the situation serves as a reminder that the confidentiality and security of legal records remain a critical component of the justice system.