OpenVoiceNews U.K.

Transparent. Unbiased. Yours.

Cyberattack on Legal Aid Agency Exposes Nearly Two Decades of Applicant Data

August 5, 2025

Categories: Breaking News

Download IPFS

A serious cyberattack targeting the Legal Aid Agency (LAA) has compromised sensitive personal data from users who accessed its digital services over the last 18 years, the

Ministry of Justice (MoJ) has confirmed. The breach has prompted a multi-agency investigation and raised broader concerns about the security of government-managed digital systems.

In a press release issued on 19 May, the MoJ revealed that the breach was first discovered on 23 April, when the LAA identified unusual activity within its internal network. The agency quickly launched a full-scale investigation, enlisting cybersecurity specialists to assess the nature and scope of the incident. The breach has since been reported to the National Crime Agency (NCA), the National Cyber Security Centre (NCSC), and the Information Commissioner's Office (ICO).

By 16 May, it became clear that the breach was far more extensive than initially suspected. According to the MoJ, the attackers had successfully accessed and extracted large volumes of personal data belonging to legal aid applicants who used the LAA's digital service from as early as 2007 through to 16 May 2025, when the affected systems were taken offline.

In an update published by the LAA, the agency acknowledged that cyber criminals had stolen contact details, addresses, dates of birth, national identification numbers, and criminal history records. Additionally, employment information and financial data, including contributions, outstanding debts, and payment records, were also compromised.

The LAA is urging all individuals who applied for legal aid during this 18-year window to exercise caution. It advised users to remain alert for suspicious activity, change account passwords, and verify the legitimacy of requests before disclosing personal information. Legal aid providers have also been notified that some of their information may have been affected.

To prevent further misuse of the stolen data, the LAA has obtained an injunction banning its distribution. Any breach of this order could result in imprisonment.

The incident highlights growing vulnerabilities in government infrastructure and the long-

term implications of insufficient data safeguards. Although digital transformation has improved access to services, it also presents significant risks if robust security protocols are not maintained.

The LAA has pledged to enhance its system protections and ensure lessons are learnt from this breach. Meanwhile, oversight bodies are continuing to investigate the source of the attack and the potential exposure of sensitive legal information.