



Media Relations
publicinfo@lacourt.org

FOR IMMEDIATE RELEASE:
July 29, 2024

SUPERIOR COURT OF LOS ANGELES COUNTY RETURNS TO NORMAL OPERATIONS FOLLOWING RANSOMWARE ATTACK

The Superior Court of Los Angeles County has restored all public-facing and internal network systems following a July 19 ransomware attack that rendered many of the Court's systems inaccessible, Presiding Judge Samantha P. Jessner and Executive Officer/Clerk of Court David W. Slayton announced today.

"I remain grateful for the patience demonstrated by court users and the legal community over the past week. The Court's dedicated and determined staff worked with outside experts and law enforcement to expeditiously restore our systems that were critically impacted by the ransomware attack," Presiding Judge Jessner said. "As of this morning, all of the Court's primary systems are fully functional and timely and efficient access to justice for Los Angeles County residents has been restored."

The Court has reinstated full access to more than 15 public-facing services, allowing court users to appear in court remotely, access all available documents in all litigation types, register for jury duty through the MyJuryDuty Portal, make traffic ticket payments or file documents online, among other services. For more details on restored services, visit the Court's [Temporary Information Center](#), which has tracked the restoration of court services in real-time since its launch last Wednesday. An indication of the significant progress the Court made over the weekend is reflected on the Temporary Information Center, which shows all the colored indicators in the news center associated with public-facing systems as "green," representing full functionality.

"It was no easy undertaking to bring all of the Court's key systems back to full functionality, but understanding the critical role the Court plays in the lives of Los Angeles County residents, our Court's talented Court Technology Services (CTS) team, as well as countless others, worked tirelessly, sometimes for days and nights on end, to bring these services back as quickly as possible," said Executive Officer/Clerk of Court David W. Slayton. "The average downtime associated with a ransomware attack can span weeks at a time. Despite that standard, I am proud the Court was able to resume basic functionality in just five days and restore the Court to full operations in just 11 days from the initial attack. I am tremendously impressed by Court staff at all levels, who continue to prove

time and time again their dedication to the Court's mission and embody what it means to be a public servant."

Court operations were severely hampered beginning in the early morning hours of Friday, July 19, when the [ransomware attack](#) was first detected. With many systems inaccessible, the Court was [forced to close](#) on Monday, July 22, to enable court staff and outside experts to focus on restoring key systems. The Court reopened on Tuesday, July 23, with a gradual restoration and resumption of services. Many essential matters were heard, including jury selection and the hearing of temporary restraining order requests, among other substantive proceedings.

Local, state and federal law enforcement agencies continue to investigate the scope and scale of the breach, as well as whether data was compromised. The forensic investigation is ongoing, and the Court will not comment further until additional information is available for public release in close consultation with law enforcement.

Follow the Court on 'X', [@LASuperiorCourt](#), and on Instagram, [@LASuperiorCourt](#), for the latest updates.