



Office of the Los Angeles City Attorney
Hydee Feldstein Soto

REPORT NO. R26-0231
04/17/2026

**REPORT IN THE PUBLIC INTEREST RE:
CYBER INCIDENT INVOLVING A CITY ATTORNEY FILE-SHARING PLATFORM**

The Honorable City Council
City of Los Angeles
Room 395, City Hall
200 North Spring Street
Los Angeles, California 90012

Honorable Members:

The Office of the Los Angeles City Attorney was the victim of a malicious cyber incident. This report will inform this Honorable Body and the public of the nature of the incident, and the steps the Office has taken, and is continuing to take, to address the incident, notify organizations and individuals whose information was involved, and ensure the security of data the Office handles.

INCIDENT OVERVIEW

The incident involved unauthorized access to a third-party, cloud-based file-sharing tool that the Office used to transfer discovery and other materials to counsel, litigants and expert witnesses in civil matters involving the City. Because the tool was used specifically for the exchange of civil litigation materials, the information generally would be limited to information provided to other parties, outside counsel or experts in civil discovery and civil litigation. The specific items in the application involved in the incident are under review and being analyzed internally and externally for identification, completeness and accuracy. As set forth below, our Office has confirmed that the incident was contained to that third-party environment, and that no other City applications, systems, or department records were accessed or affected.

RESPONSE TIMELINE

On Friday, March 20, 2026, just as Council had started a two-week recess, the City's Information Technology Agency (ITA) notified first the Los Angeles Police Department (LAPD), then the Mayor's Office and third, our Office of an apparent incident involving data maintained by our Office in the third-party file-sharing tool. The Office acted immediately to confirm the incident, secure the file-sharing tool, and investigate the scope of the incident and data involved. On the day of the incident, and over the initial weekend and the days that followed, the Office immediately coordinated closely with the ITA, the LAPD, and the Mayor's Office to implement the Office's cyber incident response plan to address the incident. This included reporting the incident to the Federal Bureau of Investigation ("FBI") on the day of the incident. In parallel, as of last week, detectives from the LAPD completed a crime report and are coordinating with the FBI on its investigation. The Office is continuing to work cooperatively with the FBI, which is leading the criminal investigation, and with the other departments in the City

Furthermore, the Office promptly engaged outside counsel with experience and expertise on cybersecurity incidents to oversee the investigation and advise on the City's legal obligations, including notification obligations under California Civil Code section 1798.29 and other applicable laws. Outside counsel, in turn, retained an external forensic firm on behalf of the Office to independently assess the incident and systems involved. On April 3, 2026, that independent forensic investigation confirmed that the incident was contained to the third-party file-sharing tool in our Office and did not involve any other City systems or data.

The Office, in collaboration with outside experts, has taken immediate steps to secure the affected environment and has implemented additional measures to enhance the file-transfer processes and to help prevent a similar incident from occurring.

ANALYSIS OF INFORMATION INVOLVED

Since first learning of the incident, our Office has worked diligently with internal stakeholders, outside counsel, external experts, and law enforcement to determine the type and amount of information involved in the incident. This work has included: (1) completing an independent forensic review of the incident to confirm the incident timeline and data involved; (2) analyzing the list of files taken to assess the specific type and amount of data involved and related cases; (3) conducting an ongoing manual review of relevant case files; and (4) implementing a process with external data analysis experts to comprehensively review file contents for potential notice obligations. While the comprehensive data analysis is in progress, the Office is continuing our internal manual review of relevant case files to assess the data involved. Our Office is working as expeditiously as possible to complete this two-part review and address applicable notice obligations.

Throughout our investigation and data review, the threat actor posted several versions of the data involved on its dark web site (a public but unindexed and hidden part of the internet accessible only through specialized browsers). After sharing small samples between March 20–27, the threat actor published the full data set, approximately 7.7 TB, on March 27 at around 3:00 a.m. PDT, where

The Honorable City Council
City of Los Angeles
April 17, 2026
Page 3

it remained for about eight hours before being taken down. The complete data set reappeared on April 3, disappeared again, and then resurfaced on the morning of April 16, 2026. Our Office, along with external advisors, has monitored these changes throughout the investigation.

NOTIFICATIONS

The Office will provide notification, as required by state law, directly to all persons whose information is determined to have been involved in the most expedient time possible and without unreasonable delay, consistent with the time reasonably necessary to complete the review described above and verify the information involved. Given the volume of material at issue, this review is substantial and is expected to take additional time to complete. As part of the notification process, the Office will also provide individuals with information and protective guidance appropriate to the specific information identified as relating to them.

Our Office provided a confidential report (R26-0189) to City Council on Friday, April 10, 2026, in anticipation of Council's return from its two-week recess, which report contained detailed information for the purpose of advising the Council of the nature of the incident and the Office's steps to address it. In response to a letter sent to our Office from the Los Angeles Police Protective League (LAPPL) asking for additional information related to the incident, a responsive letter to the LAPPL, attached to this report as an exhibit, will be provided concurrently with the filing of this report to City Council.

As we complete our review and address notice obligations, our Office will continue to coordinate with key stakeholders and provide updates to our clients and the public as appropriate.

Sincerely,



Hydee Feldstein Soto
Los Angeles City Attorney

Attachment

ATTACHMENT



Office of the Los Angeles City Attorney
Hydee Feldstein Soto

April 17, 2026

VIA EMAIL

Robert. R. Rico
General Counsel
Los Angeles Police Protective League
1308 West Eight St 4th Floor
Los Angeles, California 90017
Email: robertrico@lapl.org

Re: Malicious Cyber Incident

Dear Mr. Rico:

Thank you for your April 10, 2026 letter and for the opportunity to provide the Los Angeles Police Protective League with additional information regarding the Office of the Los Angeles City Attorney's response to the recent suspicious activity incident. The Office shares the League's interest in ensuring that any individual whose information may have been involved, including LAPD officers, receives timely and accurate notice consistent with California law.

Overview of the Incident and the Office's Response

The incident involved unauthorized access to a third-party, cloud-based file-sharing tool that the Office used to transfer discovery materials to counsel and litigants in matters involving the City. Because the tool was used specifically for the exchange of litigation materials, any officer information involved would generally be limited to officers connected in some way to litigation handled by the Office. The Office has also confirmed that the incident was contained to that third-

party environment and that no other City applications, systems, or department records were accessed or affected.

Upon first learning of suspicious activity on March 20, 2026, the Office acted immediately to secure the system involved and begin investigating. Over the initial weekend and the days that followed, the Office coordinated closely with the City's Information Technology Agency, the Los Angeles Police Department, the Mayor's Office, and the Federal Bureau of Investigation, to which the matter was promptly reported. The Office has been working cooperatively with the FBI, which is leading the criminal investigation, since that time.

The Office also promptly engaged outside counsel to oversee the investigation and advise on the Office's legal obligations, including its notification obligations under California Civil Code section 1798.29 and other applicable laws. Outside counsel, in turn, retained an external forensic firm on behalf of the Office to independently assess the incident and systems involved. That forensic investigation has confirmed that the incident was contained to the third-party file-sharing tool and did not involve any other City systems or data.

In addition to the immediate steps taken to secure the affected environment, the Office—working with its outside experts—has implemented additional measures to secure the Office's file-transfer processes and to help prevent a similar incident from occurring.

Determining the Scope of the Breach and Notification

The Office understands and shares the League's interest in ensuring that notice is provided to individual officers as quickly as possible.

The Office has prioritized its review, with assistance from necessary third parties, to determine the scope of the breach. The Office will provide notification directly to all Californians whose information is determined to have been involved, including LAPD officers, in the most expedient time possible and without unreasonable delay, consistent with the time reasonably necessary to complete that review.

With respect to that review process, we confirm that:

1. Analysis of the data involved began immediately upon the Office's discovery of the incident and has continued without interruption since that time; and
2. The Office is working through a comprehensive review of the affected data together with its outside experts to identify the specific information involved and to prepare the information necessary to notify affected individuals directly.

Given the volume of material at issue, this review is substantial and is expected to take additional time to complete. As part of the notification process, the Office will also provide individuals with information and protective guidance appropriate to the specific information identified as relating to them.

Information of Interest to the LAPD

Separate from its notification obligations under California law, the Office is also continuing to coordinate directly with the LAPD to address any questions it may have, and is sharing information with the LAPD as appropriate as the review progresses.

Point of Contact

Should the League have additional questions regarding this matter, you may contact me directly.

Sincerely,

Denise C. Mills

Denise Mills
Chief Deputy City Attorney