



[Press Releases](#)

April 29, 2021

ATTORNEY GENERAL'S OFFICE ISSUES PUBLIC NOTIFICATION OF NETWORK COMPROMISE

Raoul Establishes Toll-Free Hotline and Provides Online Information to Residents

Chicago —Attorney General Kwame Raoul today announced the Office of the Attorney General is [notifying the public](#) in accordance with state statute, of a ransomware attack that has compromised the office's network. While the extent of the information compromised is currently under investigation, the Attorney General's office is launching a toll-free hotline and providing additional information to the public via its website.

The Attorney General's office, aided by law enforcement and external technology experts, continues to evaluate the full extent of the compromise, including identifying the information that was exposed and what was done with that information. At the same time, work is taking place around the clock to rebuild the office's network. In the interim, the Attorney General's office is launching a hotline that will go into operation at 8 a.m. Central time Friday. The Attorney General's office is providing additional information to answer individuals' questions and help them protect against identity theft.

"While we do not yet know with certainty what was compromised in the ransomware attack, we are working closely with federal law enforcement authorities and outside technology experts to determine what information was exposed, how this happened, and what we can do to ensure that such a compromise does not happen again," Raoul said. "This process will take time, but I understand that members of the public may have questions now, which is why I am establishing a toll-free hotline and making information available online. I am committed to transparency throughout this very sensitive process and will continue to provide updates that do not jeopardize the progress of our ongoing investigation or the security of our network."

What has since been identified as a ransomware attack was initially discovered in the early hours of Saturday, April 10 when employees were unable to access the office's network. The office launched an immediate investigation and has maintained close contact with federal law enforcement and external technology experts to determine which network components have been compromised. The office has continued regular operations to the extent possible while efforts to rebuild the network are underway.

Illinois statute requires residents to be notified if their information may have been compromised by a data breach. Accordingly, a [public notification](#) and answers to [frequently asked questions](#) related to the network compromise are now available on the Attorney General's website. The Attorney General's office has not yet determined what personal information on its network is impacted. However, information from the public stored on the office's network includes names, addresses, email addresses, Social Security numbers, health insurance and medical information, tax information, and driver's license numbers. The Attorney General's office routinely offers guidance to help residents protect themselves from identity theft, and today's public notice details steps people can take to protect their identities.

Attorney General Raoul also announced a dedicated toll-free hotline staffed by Rust Consulting Inc., a company that specializes in legal notifications. Beginning Friday, individuals who have questions about the network compromise can call the Attorney General's Computer Network Compromise Hotline at 1-833-688-1949, Monday through Friday between the hours of 8 a.m. and 5 p.m. Central time.

The Attorney General's office continues to evaluate the extent of the network compromise by ransomware. Additional details about the compromise and the personal information impacted will be made available on the Attorney General's website, to the extent possible, upon completion of the office's internal investigation and its work with law enforcement and external technology experts.

Please see the attached Important Notice from the Illinois Attorney General Regarding Computer Network Compromise, which can also be found on the [Attorney General's website](#).



Important Notice from the Illinois Attorney General Regarding Computer Network Compromise

On the morning of Saturday, April 10, the Attorney General's office discovered that the office's computer network had been compromised by a ransomware attack. The Attorney General's office began an immediate investigation and continues to work closely with law enforcement authorities to determine the extent of the compromise, what information was exposed, and what was done with the information on its system. The Attorney General's office will provide updates, to the extent possible, upon completion of its ongoing internal review, aided by external technology experts.

Information Impacted

At this point, the Attorney General's office cannot state with certainty what information has been impacted. However, the following types of personal information from the public are held on the office's network and may be impacted:

- Names.
- Addresses.
- Email addresses.
- Social Security numbers.
- Account number or information.
- Health insurance information and records.
- Medical information.
- Tax information.
- Driver's license numbers.
- Other such information as necessary to accomplish the duties within a division or bureau of the Office of the Illinois Attorney General.

Individuals Impacted

The review is ongoing, and the Attorney General's office has not yet concluded exactly what personal information on its network is impacted and what individuals are affected. Not all records held by the Attorney General's office contain all the types of information listed above. Additional details regarding the compromise and what personal information was affected, will be made available to the extent possible upon the conclusion of the office's ongoing internal review

and work with external technology experts. Available updates will be posted on the Illinois Attorney General webpage: www.illinoisattorneygeneral.gov.

Frequently Asked Questions

FAQs can be found on the Attorney General's website here:

https://illinoisattorneygeneral.gov/consumers/publicnotice/OAG_Network_Compromise_FAQ_04_29_21.pdf

The information will be updated as more information is obtained through the office's internal review and work with law enforcement and external technology experts.

Dedicated Hotline

The Illinois Attorney General's office has established a toll-free hotline to assist in answering questions about the computer network compromise. Individuals can call 1-833-688-1949 between the hours of 8 a.m. and 5 p.m. Central time, Monday through Friday.

Identity Theft Protection Tips

Fraud Alert

- If you have shared information with the office, you may want to consider placing a fraud alert on your credit report:
 - Contact one of the three major consumer reporting agencies: TransUnion, Equifax, or Experian. The agency you contact will share the information with the other two consumer reporting agencies.
 - Fraud alerts act as a red flag to potential credit grantors indicating that they should ask for additional information in order to verify the credit applicant is you and not an imposter.
 - Fraud alerts last for one year.
 - A fraud alert does not impact your credit report or the credit score derived from data within your credit report.

General Identity Theft Protection Tips

The Attorney General's office frequently makes the following recommendations and encourages people to consider taking these actions to help secure their personal identities:

- Consider freezing (also known as a security freeze) your credit reports:
 - You must contact all three major consumer reporting agencies separately to request a freeze.
 - A freeze prevents a potential credit grantor from seeing your credit report until you verify your identity with individual consumer reporting agencies and confirm that it really is you, and not an imposter, applying for credit.
 - Credit freezes are free to place and lift.
 - A credit freeze does not impact your credit score, and it must be lifted in order to apply for credit or a loan.

- Review your credit reports, and promptly dispute any inaccurate entries with both the consumer reporting agency and the creditor:
 - Visit annualcreditreport.com or call 1-877-322-8228 to obtain your free reports. Normally, you are entitled to three free credit reports per year. However, during the COVID-19 pandemic, you can obtain a free credit report each week through April 20, 2022.
 - Going to annualcreditreport.com or calling this toll-free number is the **only** way to be sure you won't be charged for your free credit reports. Other websites try to sell you additional products or services that are not required in order to obtain a free credit report.

- View your financial account statements at least once a month, if not more frequently, and promptly dispute any unauthorized transactions with your bank.

- Place transaction alerts with your bank:
 - Ask your bank to notify you when more than a pre-set amount that you choose is charged to your account. For example, if you set an alert for \$25 or higher and you withdraw \$40 from your account, you will receive notification of the \$40 transaction.
 - If you receive notification of a transaction you did not initiate, you should dispute it immediately with your bank.
 - Transaction alerts can be configured to provide text message and/or e-mail message alerts.

- Take note of unusual events and act promptly:
 - If you receive a message from your email provider or phone service provider stating that you recently changed your mailing address or reset your password, but you did not do so, tell your provider right away that you did not make the change.
 - Never respond to emails or phone calls requesting account or identity verification that you did not initiate. Legitimate businesses will never solicit password information over email. If you have any doubt as to the legitimacy of any correspondence, hang up the phone or ignore the email and instead call the business or institution directly to verify the correspondence you have received.

- To contact the consumer reporting agencies to place or obtain more information about a fraud alert or credit freeze:
 - Equifax
 - www.equifax.com/personal/
 - P.O. Box 105788, Atlanta, GA 30349
 - 1-800-525-6285 (fraud alert)
 - 1-888-298-0045 (credit freeze)

- Experian
 - www.experian.com
 - P.O. Box 9554, Allen, TX 75013
 - 1-888-397-3742 (fraud alert)
 - 1-888-397-3742 (credit freeze)
- TransUnion
 - www.transunion.com
 - P.O. Box 2000, Chester, PA 19016
 - 1-800-680-7289 (fraud alert)
 - 1-888-909-8872 (credit freeze)
- To contact the Federal Trade Commission for more information about a fraud alert or credit freeze, or to learn about additional identity theft resources:
 - www.ftc.gov
 - [Identity Theft Recovery Steps | IdentityTheft.gov](http://IdentityTheftRecoverySteps.IdentityTheft.gov)
 - Federal Trade Commission, 600 Pennsylvania Ave, NW, Washington, D.C. 20580
 - 1-877-382-4357 (Consumer Help Line)
- If you still have questions or concerns, you can find more information on the Attorney General's website:
 - Identity theft resources and details on how to place a fraud alert or credit freeze can be found at [Illinois Attorney General - Protecting Consumers - ID Theft Hotline](#).
 - Updates to the information provided in this notice will be posted on www.illinoisattorneygeneral.gov.