Office of the Illinois Attorney General Computer Network Compromise
Frequently Asked Questions
April 29, 2021

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.

Below are answers to frequently asked questions. If you would like to speak with someone about your questions, the Illinois Attorney General's office has established a toll-free hotline that will be available Monday through Friday from 8:00 a.m. to 5:00 p.m. Central time.
The number is **1-833-688-1949.**

1. What happened to the Office of the Illinois Attorney General's network?

The Office of the Illinois Attorney General's network has been compromised by a ransomware attack. The office is still in the process of investigating and determining the extent of the compromise, what information was exposed, and what was done with the information on its system.

2. What does this mean for my personal information?

At this point, the office does not know with certainty what information has been impacted. However, the following types of personal information from the public are held on the office network and may be impacted:

- Names.
- Addresses.
- E-mail addresses.
- Social Security numbers.
- Account numbers or information.
- Health insurance information and records.
- Medical information.

- Tax information.
- Driver's license numbers.
- Other similar information as necessary to accomplish the duties within an attorney general division or bureau.

3. How was the Illinois Attorney General's office network compromised?

The Office of the Illinois Attorney General's network has been the victim of a ransomware attack. The office is still in the process of investigating and determining how the network was compromised, the extent of the compromise, what information was exposed, and what was done with the information on its system.

4. What is a ransomware attack?

A ransomware attack occurs when a malicious actor gains unauthorized access to a computer network. After gaining access to the network, the malicious actor launches ransomware malware to block the rightful owner's access to all data held within the network, and keeps access blocked unless the rightful owner pays a specified amount of money. However, there is no guarantee that full access will be restored even if payment is made.

5. Did the Illinois Attorney General's Office pay to regain access to its system?

The office is still in the process of investigating the ransomware attack, and currently is not able to share additional details. When the office has additional information that can be shared without compromising the investigation or further risking the integrity, security, and confidentiality of the system, that information will be provided on the office's website: www.illinoisattorneygeneral.gov.

6. Why did the Illinois Attorney General's office notify the public about this compromise?

The Illinois Attorney General's office issued a public notice about its network being compromised by a ransomware attack because the network holds personal information belonging to members of the public.

The Illinois Attorney General's office is still in the process of investigating and determining the extent of the compromise, what information was exposed, and what was done with the information on its system.

Because the office does not yet know what information was exposed, it is not able to provide additional specific information or contact specific impacted individuals at this time. However, the Illinois Attorney General's office wants the public to have information about the compromise that can be shared currently so that individuals who believe their personal information may be impacted are aware of the situation and can take appropriate steps to protect their personal identities.

7. Why can't you look up a complaint or inquiry I made to the Attorney General's office?

Because of the ransomware attack to its computer network, the Illinois Attorney General's office does not yet have full access to its system. Until the office is confident that the security and integrity of its network has been restored, the Attorney General's office will keep all constituents' personal information in an offline format only.

8. Why don't you know whether my information was compromised or what information was compromised?

The Illinois Attorney General's office is still in the process of investigating and determining the extent of the compromise, what information was exposed, and what was done with the information on its system.

9. When will you know more about what happened and whether my information was compromised?

The Office of the Attorney General's investigation and internal review are ongoing. When the office learns more about what happened, including what happened to the personal information on its network, it will update the information on its website: www.illinoisattorneygeneral.gov.

10. Do I need to do anything in response to this notice?

This notice does not require you to take any action. This notice is meant to inform the public about the computer network compromise and provides information about the office's ongoing internal review and investigation.

11. Do I need to do anything to protect my personal identity because of this incident?

If you have provided personal information to the Illinois Attorney General's office at any time in the past, you may wish to place a fraud alert on your credit report.

If you don't believe the Illinois Attorney General's office has any of your personal information, you may still wish to follow the general tips provided to protect your personal identity.

12. What measures are in place to protect my identity and personal information?

The Illinois Attorney General's office is still in the process of investigating and determining the extent of the compromise, what information was exposed and what was done with the information on its system. The Illinois Attorney General's office also will take any necessary steps to ensure its network is secure and to minimize the risk of a future ransomware attack.

13. Should I request a fraud alert with the three major credit bureaus?

Individuals who have provided personal information to the Illinois Attorney General's office in the past may consider requesting a fraud alert on their credit report. A fraud alert is a message that credit issuers receive when someone applies for new credit in your name. The message tells

creditors that there is possible fraud associated with the account and gives them a phone number to call (yours) before issuing new credit. You can contact the fraud department at any one of the three major credit bureaus:

- Trans Union: 1-800-680-7289 (http://www.transunion.com)
- Experian: 1-888-397-3742 (http://www.experian.com)
- Equifax: 1-888-525-6285 (http://www.equifax.com)

As soon as one credit bureau confirms your fraud alert, the other two credit bureaus will be automatically notified to place fraud alerts.

You should be aware that a fraud alert may make it more difficult for you to obtain credit or process financial transactions, and you should exercise caution in doing so. While it will not affect your credit, it will slow down the credit application process.

14. What other things can I do to protect my identity from identity thieves?

The Attorney General's Office frequently provides tips to the public and encourages people to consider taking these actions to help secure their personal identity. In addition to placing a fraud alert, you may wish to consider taking the following steps.

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

- To contact the credit bureaus to place or obtain more information about a credit freeze:
    - Equifax
        - 1-888-298-0045 (credit freeze)
        - www.equifax.com/personal/
    - Experian
        - 1-888-397-3742 (credit freeze)
        - www.experian.com
    - TransUnion
        - 1-888-909-8872 (credit freeze)
        - www.transunion.com

- Review your credit reports, and promptly dispute any inaccurate entries with both the credit bureau and the creditor:
    - Visit to annualcreditreport.com, or call 1-877-322-8228 to get 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 be notified 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 a call or email, hang up the phone or ignore the email and instead call the business or institution directly to verify the message you have received.

15. What should I do if I am contacted by someone who identifies themselves as acting on behalf of the Illinois Attorney General?

The Illinois Attorney General's office has not contacted any member of the public directly about the network compromise. Unless you have been told that a representative of the Attorney General's office will be contacting you regarding a specific question you've asked, please do not provide any information to someone who contacts you about the office's network compromise.

16. Can I talk with someone if I have questions?

The Illinois Attorney General's office has established a toll-free hotline available Monday through Friday from 8:00 a.m. to 5:00 p.m. Central time to assist in answering questions about the computer network compromise. That number is **1-833-688-1949**.