CITY OF LONG BEACH

April 2025

Network Security Incident Update
Frequently Asked Questions

What happened?
The City values and respects the personal information it maintains and is committed to being open and transparent with the community. The investigation into the network security incident that occurred on or about Nov. 14, 2023, has revealed that files containing certain personal information were accessed and/or acquired. The City is now in the process of notifying people whose personal information may have been accessed and/or acquired and is sending letters via U.S. mail to those impacted. While there is no indication that any information has been misused for the purpose of committing fraud or identity theft, the City is providing these notifications out of an abundance of caution, and pursuant to law, so that those impacted have the information, tools and resources to safeguard their personal information.

What information was involved?
The potentially impacted files contained first and last names in combination with one or more of the following: date of birth, financial account information, credit and/or debit card information, Social Security number, biometric information, medical diagnosis and/or treatment information, medical provider information, health insurance information, driver's license number, passport number, medical record number, taxpayer identification number, and patient account information. The types of personal information involved varied by individual and not every data element was impacted for each individual.

What is the City of Long Beach doing about this?
The City is in the process of sending notification letters via U.S. mail to people who may be affected using their last known home address that is available to the City. The letters explain the services available to potentially affected individuals and provide tools to help safeguard against identity fraud. The City is also disclosing this same information on longbeach.gov to ensure it is publicly accessible for all who believe they should have received a notification letter and have not. The City has also established a dedicated call center staffed with professionals familiar with this incident to provide information and resources. The call center is available at 888.802.9667, Monday through Friday, 6 a.m. to 6 p.m. Pacific Time, excluding holidays. The City is also offering people whose Social Security numbers were potentially impacted with complimentary credit monitoring services in accordance with applicable state laws.

Are the City's systems safe to use?
Yes, the City's systems have been and remain safe to use. When the City first learned of the network security incident that occurred on or about Nov. 14, 2023, out of an abundance of caution, the City took certain systems offline for a temporary period for the initial investigation and remediation. During this time, most core City services were unaffected and continued to operate normally. All impacted systems were restored over the subsequent weeks.

Why did it take so long to notify impacted individuals?
The investigation of the network security incident has been ongoing since November 2023 and included an extensive forensic investigation and manual document review, which took approximately 15 months to complete. Anyone who has experienced a sophisticated cyber incident knows it is a time-intensive process. We take the security of information very seriously and needed to be sure we were confident in the results of the investigation before making any notifications. In accordance with direction from its outside legal counsel and data privacy experts, and in alignment with cybersecurity best practices, the City concluded the investigation and it was determined the names of those who were potentially compromised along with what type of data may have been accessed and/or acquired.

How will I know if my information was compromised?

Those impacted will receive a letter from the City of Long Beach via U.S. mail. If people believe they may have been impacted and did not receive a notification letter, or have any further questions regarding this incident, they should call our dedicated toll-free response line at 888.802.9667.

Why did I receive a notification from the City?

You received a notification because the investigation determined that your personal information may have been access and/or acquired. Protecting the privacy and security of your information is a top priority for the City. The City respects and values your privacy, which is why it is notifying you about the incident to ensure you are aware and have the information and resources to safeguard information, should you choose to do so.

I received a notification from the City about a security incident. Does this mean someone has misused or will misuse my information?

The City is not aware of any reports of fraud arising out of this incident. The City provided you with a notification letter to make you aware of the incident and provide you with guidance on what you can do to further protect yourself.

Is the City providing credit monitoring services?

The City is offering credit monitoring to individuals whose Social Security numbers were potentially affected.

What can I do to protect myself?

The City encourages people to take the following precautionary measures:

- Carefully review the letter you received for steps you can take to protect yourself. The notice contains information about the incident, our response, and information and resources to help you protect your information.
- Enroll in the credit monitoring services offered at no cost to you, if eligible.
- You should always remain vigilant against incidents of identity theft and fraud by reviewing your financial account statements and monitoring your free credit reports to detect errors or identify suspicious activity.
- You may consider placing a fraud alert and/or security freeze on your credit file.
- You may order a free credit report.

Where do I file a police report?

If there is reason to believe your personal information has been used to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts.

- Long Beach residents can obtain a police report by calling the Long Beach Police Department non-emergency line at 562.435.6711.
- People may also file a complaint with the FTC online, by phone at 1.877.IDTHEFT (1.877.438.4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

How much is this costing Long Beach taxpayers?

Most costs incurred as a result of this incident were absorbed in the operating budget of the General Services Fund (an internal service fund) in the Department of Technology and Innovation.

What are you doing to ensure this doesn't happen again?

We take the privacy and security of the information entrusted to us very seriously. While we have safeguards in place to protect the data in our care, we are working to review and further enhance these protections. We are taking the necessary steps to best prevent a similar incident from occurring in the future.

Long Beach continues to invest each year to enhance cybersecurity measures. As part of the City's Adopted Fiscal Year 2025 Budget, $1 million was added to enhance cybersecurity and information technology infrastructure through the use of cybersecurity experts, training, testing, data loss prevention tools, and more. The City continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains and requires all City employees to complete an annual mandatory cybersecurity awareness training, among other safeguarding techniques.

How did the unauthorized user (threat actor) gain access to the City's network? Why didn't the City take precautions to prevent this from occurring?

We cannot disclose specific details due to security considerations, as sharing such information could expose vulnerabilities that may attempt to be exploited further. The City has and will continue to invest in cybersecurity measures. Additionally, we want to assure the public that the City took immediate action to contain the incident, further strengthen our defenses, and worked with cybersecurity experts to prevent future occurrences. Protecting our systems and the information entrusted to us remains our highest priority.

Where can I learn more about the network security incident?

More information about the network security incident is available at longbeach.gov/networksecurityincident. More information about the investigation update is available via the homepage of the City's website at longbeach.gov.

When will another update be made?

Since the investigation of the network security incident has now concluded, this is considered the final foreseeable update on the matter.

I have other questions, what should I do?

People with additional questions should call the dedicated call center at 888.802.9667. The call center is staffed with professionals familiar with this incident to provide information and resources. The call center is available Monday through Friday, 6 a.m. to 6 p.m. Pacific Time, excluding holidays.

I do not speak English. Are there language interpretation services available?

People requiring language interpretation should call the call center number, available at 888.802.9667, and they will be connected to interpretation services.