City of Gloversville

3 Frontage Road
Gloversville, New York 12078-2897
518-773-4500 (phone) 518-773-2593 (fax)

FOR IMMEDIATE RELEASE

October 25, 2025

The city computer network sustained a Ransomware Attack which was discovered by our Finance Commissioner, Tammie Weiterschan on Friday morning March 14, 2025. A ransom note was found on the server with instructions on how to negotiate with the Threat Actor Group later believed to be from Eastern Europe.

She immediately notified the Mayor, Police Chief Michael Garavelli and all members of the city council. That same morning, the police chief and the finance commissioner reported the incident to:

1. The NYS Dept of Homeland Security' Cyber Incident Response Team (CIRT)
2. The NYS Police Cyber Analysis Unit (CAU)
3. The FBI

CIRT met with city officials that afternoon regarding the appropriate response to the incident.

Since this was an active criminal investigation, it remained confidential, on a need-to-know basis, per the recommendation of State and Federal law enforcement agencies assisting the city. (FBI, Dept of Homeland Security, US Secret Service, NYS Police)

The City IT provider and the Police Department IT provider immediately began remediation and recovery efforts that continued non-stop through the weekend and into the following weeks.

Tuesday, March 18 CIRT strongly recommended that the city retain a Cyber Incident Response and Security Firm and a legal firm that specialize in handling these incidents.

The following day, the City contacted and subsequently retained both a Cyber Security and Forensic Technology Firm and the legal firm of Harter, Secrest and Emery, LLP. To assist in investigation and recovery.

Our consultants immediately began negotiations with the Threat Actor Group to reach a settlement which would recover the stolen data since the attack compromised the personal identifying information of all city employees, current and retired, including payroll records, direct deposit information and account numbers.

Meanwhile, the city took steps immediately to safeguard and secure any other sensitive information from further compromise and made all notifications in accordance with the law. The city sent out over 3,000 letters notifying all current and former employees and any members of the

general public that were at risk of having their personal information compromised. These notifications offered credit monitoring services and Identity Theft Protection for one year at no

cost to the affected individuals. The city also notified the Attorneys General of nine states as required by law.

Based on the recommendations of our legal and cyber security experts, the decision was made and approved by the City Council to pay the ransom to the Threat Actor Group and recover the data. The original demand from the Threat Actor Group was $300,000. The amount paid was $150,000. The stolen data was de-encrypted and fully recovered.

The city was advised that the FBI had been able to track these transactions in the past. This incident possessed certain characteristics that might allow it to be tracked, the ransom recovered, and the suspects caught. Accordingly, there is still an open investigation into this incident along with the incidents suffered by several other cities and businesses in the region that were perpetrated by the same group.