THE CLERKS AUTHORITY
Georgia Superior Court Clerks' Cooperative Authority

**PRESS RELEASE**

**For Immediate Release:**
**November 28, 2025**

**Contact: Mike Smith**
**(404) 327-9058**

# Statement on Recent Outage

**Atlanta, GA** – During the afternoon of November 21, 2025, the Georgia Superior Court Clerks' Cooperative Authority ("GSCCCA" or "Clerks' Authority") Information Technology Team detected anomalous network behavior consistent with an active intrusion attempt. Early indicators revealed that a threat actor had gained access to the network perimeter. In alignment with established cybersecurity best practices and our internal incident-response procedures, defensive controls were immediately activated and mitigation steps initiated.

Because of the speed of our detection and response, the GSCCCA successfully interrupted a ransomware attack in progress **before any encryption, destruction, or alteration of data occurred**.

During this same period, the GSCCCA was also contacted by the FBI with information regarding a credible and imminent threat targeting our environment. Although our teams were already actively mitigating the intrusion, the FBI's alert corroborated our internal findings and underscored the seriousness of the threat. Based on both the real-time attack indicators and the additional federal intelligence, GSCCCA leadership made the difficult but necessary decision to shift into a full defensive posture. This included **temporarily restricting public access to GSCCCA websites, applications, and resources** to protect the integrity of our systems and prevent the threat actor from advancing further.

Throughout this restricted-access window, GSCCCA IT teams worked around the clock to ensure that no persistent footholds remained, to harden affected systems, and to close any defensive gaps that could enable a repeat attack. Consistent with NIST, CIS, and industry best practices for containment and eradication, more than 100 servers and workstations across the Clerks' Authority were **individually inspected and scanned in isolated environments** prior to being returned to service. This was a time-consuming but essential step to ensure complete eradication of the threat.

At this time, the GSCCCA confirms that the threat has been fully neutralized and that all GSCCCA systems have been safely reverted to normal operation.

During this process, the Authority received a ransom demand associated with claims of data theft and encryption. The GSCCCA did **not** engage with the threat actor, and no ransom was paid. The attacker provided a screenshot purporting to show access to GSCCCA data. Our investigation confirms that the screenshot likely depicts a **development server** containing **test versions** of GSCCCA databases. These test datasets contain only a subset of production information, and numerous fields are sanitized to support integration-partner testing.

**– MORE –**

THE CLERKS AUTHORITY
Georgia Superior Court Clerks' Cooperative Authority

**Importantly**:

- The GSCCCA **does not collect or store Social Security numbers**, nor does it store bank account numbers, credit card numbers, or other cardholder financial data.
- While certain payment information is collected during transactions, **all sensitive financial data is transmitted directly to and processed by our PCI-compliant third-party payment partners**. The GSCCCA **does not retain or store** this information within its systems.
- The information contained in GSCCCA real-estate-related systems is **public record** by definition.
- At this time, the GSCCCA **cannot confirm that any data was** stolen from our systems. Forensic analysis is ongoing, and no evidence currently indicates that sensitive or non-public data was accessed or removed. The purported deadline for the supposed data leak has now passed.
- The attack was interrupted **before any encryption, destruction, or alteration of data occurred**.

We recognize that the temporary service outage was disruptive to the clerks, courts, partners, and citizens who rely on GSCCCA services every day. We sincerely apologize for this impact. However, it is important to understand that **limiting public communication during an active intrusion is itself a best practice**. Providing detailed information during an ongoing incident can unintentionally undermine containment efforts or provide actionable intelligence to the attacker.

Finally, we want to express our gratitude for your patience and understanding. Ransomware events that are not contained early often result in system-wide outages lasting weeks or even months. We are confident that the swift actions of our IT teams—and the Clerks' Authority's commitment to strong cybersecurity posture—were instrumental in protecting GSCCCA systems and ensuring their long-term availability.

###

**GEORGIA SUPERIOR COURT CLERKS' COOPERATIVE AUTHORITY**

1875 Century Blvd, Suite 100, Atlanta, GA 30345
Office: 404.327.9058 · Fax: 404.327.7877 · http://www.gsccca.org