

# Notice of Data Security Incident

Gesa Credit Union (“Gesa”) is providing notification of a recent data security incident that occurred at Marquis Software Solutions (“Marquis”), a former digital and physical marketing and communications vendor for Gesa. This incident involved information related to some of our members. However, this incident did not impact our internal network. This notice includes information about the incident, Marquis’ response, and steps potentially impacted parties may take to protect against possible misuse of their information, should they feel it necessary to do so. If an individual’s information was impacted by this incident Marquis will be mailing information to the last known address of record.

**What Happened?** On August 14, 2025, Marquis identified suspicious activity on its network and later determined that it was the result of a cybersecurity incident. Upon learning of the incident, Marquis immediately launched an investigation and engaged third-party cybersecurity specialists to assist. Marquis also notified law enforcement. Marquis’ investigation determined that an unauthorized third-party accessed the Marquis network and may have accessed and acquired certain files from its systems. Importantly, Gesa’s internal systems were not impacted; the incident was limited to the vendor’s environment.

**What Information Was Involved?** Marquis reviewed the contents of the impacted data and determined the information impacted may include our members’ first and last name in combination with one or more of the following data elements: date of birth, Social Security number, financial account information, payment card information, and/or taxpayer identification number.

**What We Are Doing.** In response to this event, Marquis has taken steps to reduce the risk of this type of incident occurring in the future. Additionally, Gesa has not had any ongoing business relationship with Marquis since 2020. Marquis is mailing notice letters to potentially impacted individuals with more information regarding this incident. If you have questions about this incident or the letter you received, please call the dedicated assistance line at [855-403-1764](tel:855-403-1764) between Monday through Friday, 9 am to 9 pm ET (excluding holidays).

**What You Can Do.** In general, we encourage individuals to remain vigilant against incidents of identity theft and fraud by reviewing credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call [1-877-322-8228](tel:1-877-322-8228).

Individuals have the right to place an initial or extended “fraud alert” on a credit file at no cost. If individuals are the victim of identity theft, they are entitled to an extended fraud alert lasting seven years. As an alternative to a fraud alert, they have the right to place a “credit freeze” on a credit report. The credit freeze is designed to prevent credit, loans, and services from being approved without consent. Pursuant to federal law, individuals cannot be charged to place or lift a credit freeze on their credit report.

Should individuals wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion	Experian	Equifax
<a href="tel:1-800-680-7289">1-800-680-7289</a>	<a href="tel:1-888-397-3742">1-888-397-3742</a>	<a href="tel:1-888-298-0045">1-888-298-0045</a>
<a href="http://transunion.com">transunion.com</a>	<a href="http://experian.com">experian.com</a>	<a href="http://equifax.com">equifax.com</a>
P.O. Box 2000	P.O. Box 9554	P.O. Box 105069
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348

Individuals can further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps to protect their personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or their state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT ([1-877-438-4338](tel:1-877-438-4338)); and TTY: [1-866-653-4261](tel:1-866-653-4261). Instances of known or suspected identity theft should also be reported to law enforcement, the state Attorney General, and the FTC.