New Hampshire Attorney General's Office
(via email)

November 26, 2025

RE: NOTICE OF DATA BREACH

Dear Attorney General,

Pursuant to the data breach notification law of New Hampshire, this letter serves as notice of a data security incident involving personal information of residents within your jurisdiction. This notification is submitted by CoVantage Credit Union ("CoVantage") on behalf of Marquis Software Solutions ("Marquis"), which is a third-party vendor of CoVantage.

Incident Description:

On August 14, 2025, Marquis identified suspicious activity on their network and determined that it was the result of a cybersecurity incident. Upon learning of the incident, they immediately launched an investigation and engaged appropriate cybersecurity experts to assist. They also promptly notified federal law enforcement. Their investigation determined that an unauthorized third party accessed their network and may have accessed and acquired certain files from their systems. The incident was limited to Marquis' environment.

Nature of Compromised Data:

On or about September 8, 2025, Marquis engaged an expert to attempt to identify the identity of specific individuals whose data was affected by the incident. Soon after receiving the results of that investigation, on or about October 27, 2025, Marquis began notifying customer data owners concerning the identities of the individuals affected and the types of compromised information. The compromised information includes: names, addresses, phone numbers, Social Security numbers, financial account information, and dates of birth. At this time, Marquis has no evidence of the misuse, or attempted misuse, of personal information as a result of this incident.

Affected Customers and State-by-State Impact:

The estimated number of affected individuals in your state by customer is as follows:

Customer Name & Address	*Number of Affected Individuals in New Hampshire*
CoVantage Credit Union 723 Sixth Ave, Antigo, WI 54409-0107	22

Remediation and Mitigation Efforts:

At the time of the incident, Marquis maintained a written information security program. Since the incident, it has enhanced its security controls in an effort to prevent future incidents by taking at least the following actions: (1) ensuring that all firewall devices are fully patched and up to date, (2) rotating passwords for local accounts, (3) deleting old or unused accounts, (4) ensuring that multi factor authentication is enabled for all firewall and virtual private network ("VPN") accounts, (5) increasing logging retention for firewall devices, (6) applying account lock-out policies at the VPN for too many failed logins, (7) applying geo-IP filtering to only allow connections from specific countries needed for business operations, and (8) applying policies to automatically block connections to/from known Botnet Command and Control servers at the firewall. Marquis is also working on: (1) rebuilding its impacted infrastructure with new Operating Systems; (2) reviewing more stringent access control policies; (3) reviewing more stringent network segmentation, and (4) deploying an Endpoint Detection and Response tool to the Marquis environment, including the implementation of alerts for: (a) IP addresses found during the forensic investigation associated with threat actor activity; and (b) malware or other suspicious files identified during the forensics investigation using hash and/or file name.

Notification to Affected Individuals:

Marquis is planning on mailing notifications to affected individuals on or around November 26, 2025. A copy of Marquis' notification letter provided to residents of your state is attached for your reference. Individuals will be provided with 24-month complimentary credit monitoring services through Epiq Privacy Solutions ID. Individuals are also being provided with a dedicated reponse line at (855) 403-1764 to have any questions answered.

Contact for Further Information:

If you require further details or assistance, please contact:

Marcus S. Zelenski, AVP Assistant General Counsel
Phone: (920) 557-0418 x5630
Email: marcus.zelenski@covantagecu.org