HONIGMAN

Steve M. Wernikoff
Office: 312.701.9380
swernikoff@honigman.com

November 26, 2025

Via Electronic Mail
Office of Attorney General of Iowa
Hoover State Office Bldg.
1305 E. Walnut St.
Des Moines, IA 50319
Email: consumer@ag.iowa.gov

Re: Notification of Data Security Incident

To Whom It May Concern:

We represent Marquis Software Solutions, Inc. ("Marquis"), a digital and physical marketing and communications vendor with a mailing address of 6509 Windcrest Dr. #170, Plano, Texas 75024. We are writing to provide notice of an incident at Marquis that may have affected the security of personal information of Iowa residents. Marquis is providing this notice on behalf of certain present and former business customers whose data Marquis has maintained, as identified below. While Marquis is submitting this notification, it does not waive any rights or defenses relating to this incident, this notice, or the applicability of Iowa law, including on personal jurisdiction. This notice will be supplemented as appropriate.

Incident Description

On August 14, 2025, Marquis detected suspicious activity on its network and determined that it was the victim of a ransomware attack. Upon discovery, Marquis promptly launched an investigation and engaged cybersecurity experts through legal counsel to assist. Federal law enforcement was also notified. The investigation revealed that an unauthorized third party accessed Marquis' network on August 14, 2025, and may have acquired certain files from its systems. The incident was limited to Marquis' environment.

Based on the forensic investigation findings, Marquis conducted a thorough review of the files potentially accessed by the unauthorized party with the assistance of a dedicated review team. The review determined that the files contained personal information received from certain business customers. The personal information potentially involved for Iowa residents includes names, addresses, phone numbers, Social Security numbers, Taxpayer Identification Numbers, financial account information without security or access codes, and dates of birth. At this time, Marquis has no evidence of misuse or attempted misuse of this personal information as a result of this incident.

Between October 27, 2025 and November 25, 2025, Marquis notified the affected business customer data owners about the potential involvement of personal information collected through them. Since then, Marquis has been working with some of these data owners – at their direction – to facilitate appropriate notifications to individuals and regulatory bodies. This notification is

submitted as part of that process and on behalf of certain present and former business customer data owners, which are listed below:

Data Owner	Number of Affected Individuals in Iowa
1st Northern California Credit Union	5
Advantage Federal Credit Union	15
BayFirst National Bank	5
Bellwether Community Credit Union	7
Community 1st Credit Union	6,511
Discovery Federal Credit Union	1
Energy Capital Credit Union	3
Founders Federal Credit Union	4
Gateway First Bank	12
Generations Federal Credit Union	4
Glendale Federal Credit Union	1
Interior Federal Credit Union	149
Kemba Financial Credit Union	20
MemberSource Credit Union	14
Michigan First Credit Union	7
New Peoples Bank	1
Pasadena Federal Credit Union	7
Texoma Community Credit Union	3
Time Bank	3,942
University Credit Union	19

To help protect affected individuals, Marquis is working with its business customers to provide appropriate consumer notification and, where applicable, complimentary credit monitoring and identity theft protection services. On November 26, 2025, data owners began providing written notice of this incident to affected Iowa residents. Notifications are expected to continue over the coming weeks. The notifications recommend that affected individuals remain vigilant for signs of identity theft or fraud by reviewing account statements and monitoring their credit reports. Information on how to take additional protective measures also is included in the individual notifications being provided by business customers. A copy of the template notification is enclosed.

Additional Steps Taken to Address the Incident

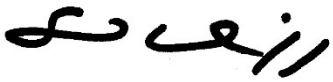
Following the discovery of the incident, Marquis took immediate steps to contain the ransomware attack, secure its network environment and identify potentially affected clients and

individuals. Since this incident, Marquis has implemented additional security technologies and processes to bolster overall security.

If you have any questions regarding this notification or need further information, please contact me using the information in the header of this letter.

Very truly yours,

HONIGMAN LLP



Steven M. Wernikoff

Enclosure: Sample Notification Letter