



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:

<i>Customer Name & Address</i>	<i>Number of Affected Individuals in New Hampshire</i>
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



Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<Date>

RE: NOTICE OF DATA <<Variable Data 1: BREACH/INCIDENT>>

Dear <<Full Name>>,

At Marquis Software Solutions (“Marquis” or “we”), a <<Variable data 2>> digital and physical marketing and communications vendor for <<Data Owner or Entity>>, protecting your personal and financial information is one of our highest priorities. We are writing to let you know about a recent data security incident that may have involved some of your information.

What Happened

On August 14, 2025, we identified suspicious activity on our network and later determined that it was the result of a cybersecurity incident. Upon learning of the incident, we immediately launched an investigation and engaged the appropriate cybersecurity experts to assist. We also promptly notified law enforcement. Our investigation determined that an unauthorized third party accessed our network and may have accessed and acquired certain files from our systems. Importantly, your financial institution’s internal systems were not impacted; the incident was limited to Marquis’ environment.

What Information Was Involved

We reviewed the contents of the copied files to determine if they contained any personal information. On October 27, 2025, we determined that the following data of yours was included in the copied files: <<Breached Elements>>. At this time, we have no evidence of the misuse, or attempted misuse, of personal information as a result of this incident.

What We Are Doing

In addition to the actions described above, we have taken steps to reduce the risk of this type of incident occurring in the future. We are also notifying you of the incident so that you can be aware and take steps to protect your information, if you feel it is appropriate to do so. Although we do not have evidence of any information potentially involved in this incident being used for unauthorized purposes, out of an abundance of caution, we are offering you a complimentary <<CM Duration>> month membership of Epiq Privacy Solutions ID. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on prompt identification and resolution of identity theft. Epiq Privacy Solutions ID is completely free to you and enrolling in this program will not hurt your credit score. For more information, including instructions on how to activate your complimentary membership, please see the additional information attached to this letter.

What You Can Do

While we have no evidence that your information has been misused, we encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity over the next 12 to 24 months. We also encourage you to take advantage of the complimentary credit monitoring included in this letter. You can also find more information on steps to protect yourself against possible identity theft or fraud on the enclosed Additional Important Information page.

For More Information

We understand this news may be concerning, and we regret any inconvenience it may cause. Our team remains committed to transparency and to protecting your information. If you have questions, please call our dedicated response line at 855-403-1764, available 9am to 9pm Eastern Time, Monday through Friday.

Sincerely,

Marquis Software Solutions, Inc.



<<Full Name>>
Activation Code: <<ACTIVATION CODE>>
Enrollment Deadline: <<ENROLLMENT DEADLINE>>
Coverage Length: <<12/24>> Months

Epiq - Privacy Solutions ID 3B Credit Monitoring

How To Enroll:

- 1) Visit www.privacysolutionsid.com and click “Activate Account”
- 2) Enter the following activation code, <<Activation Code>> and complete the enrollment form
- 3) Complete the identity verification process
- 4) You will receive a separate email from noreply@privacysolutions.com confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page
- 5) Enter your log-in credentials
- 6) You will be directed to your dashboard and activation is complete!

Privacy Solutions ID provides three bureau credit monitoring through Equifax, credit report and score access, \$1 million identity theft insurance with \$0 deductible, ID Restoration services, and dark web monitoring. See below for more details.

Credit Monitoring with Alerts

Monitors your credit file(s) for key changes, with alerts such as credit inquiries, new accounts, and public records.

3-Bureau Credit Score and Report¹

Annual 3-Bureau VantageScore and 3-Bureau Credit Report

SSN Monitoring (High Risk Transaction Monitoring, Real-Time Authentication Alerts, Real-Time Inquiry Alerts)

Real-time monitoring of SSNs across situations like loan applications, employment and healthcare records, tax filings, and payment platform, with alerts.

Dark Web Monitoring

Searches for compromised information across the dark web, with alerts.

Credit Report Lock/Freeze

Assists with blocking access to the credit file for the purposes of extending credit (with certain exceptions).

Lost Wallet Assistance

Assistance with canceling and reissuing credit and ID cards.

Identity Restoration

Dedicated ID restoration specialists who assist with ID theft recovery.

Up to \$1M Identity Theft Insurance²

Provides up to \$1,000,000 (\$0 deductible) Identity Theft Event Expense Reimbursement Insurance on a discovery basis. This insurance aids in the recovery of a stolen identity by helping to cover expenses normally associated with identity theft.

Unauthorized Electronic Funds Transfer- UEFT²

Provides up to \$1,000,000 (\$0 deductible) Unauthorized Electronic Funds Transfer Reimbursement. This aids in the recovery of stolen funds resulting from fraudulent activity--occurrence based.

Personal Info Protection

Helps users find their exposed personal information on the surface web—specifically on people search sites and data brokers – so that the user can opt out/remove it. Helps protect members from ID theft, robo calls, stalkers, and other privacy risks.

If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID, please call directly at **866.675.2006**, Monday-Friday 9:00 a.m. to 5:30 p.m., EST.

1 The credit scores provided are based on the VantageScore 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness. Credit monitoring from Experian and TransUnion will take several days to begin.

2 Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

The District of Columbia and Massachusetts law also allow consumers to place a security freeze on their credit reports. A security freeze can be placed without any charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures:

Equifax Security
Freeze 1-888-298 0045
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742
<https://www.experian.com/freeze/center.html>
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
<https://www.transunion.com/credit-freeze>
P.O. Box 160
Woodlyn, PA 19094

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>. Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax
1-866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 1000
Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

District of Columbia Residents: District of Columbia residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at 441 4th Street, NW, Washington, DC 20001, 202-727-3400, oag@dc.gov, <https://oag.dc.gov/>. The District of Columbia law also allows consumers to place a security freeze on their credit reports without any charge.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Massachusetts Residents: You may contact and obtain information from your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, <http://www.marylandattorneygeneral.gov/>.

New Mexico: Individuals have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfrp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; <https://ag.ny.gov/consumer-frauds/identity-theft>; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Oregon Residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. For more information on security locks, you can visit the Oregon Department of Consumer and Business Services website at dfr.oregon.gov/financial/protect/Pages/stolen-identity.aspx and click "Place a credit freeze."

Rhode Island Residents: We believe that this incident affected <<RI #>> Rhode Island residents. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).