



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Michele Veltri
Office: (267) 930-2297
Fax: (267) 930-4771
Email: mveltri@mullen.law

75 S. Clinton Avenue, Suite 510
Rochester, NY 14604

February 21, 2023

VIA ELECTRONIC MAIL

Office of the Attorney General
Attn.: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Marquette Management Inc. (“Marquette”) located at 135 Water Street, 4th Floor, Naperville, Illinois 60540, and are writing to notify your office of an incident that may affect the security of certain personal information relating to one (1) Maryland resident. By providing this notice, Marquette does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On November 30, 2022, Marquette was alerted that an unauthorized party had intercepted email communications between Marquette and a third party. In response, Marquette immediately took steps to secure its email tenant and launched an investigation to determine the nature and scope of the incident. This investigation recently concluded, and determined that between November 4, 2022 and December 1, 2022 an unknown, unauthorized actor gained access to one Marquette email account and potentially accessed and/or acquired certain information stored within that account.

Marquette quickly began a thorough investigation of the relevant emails and files to identify individuals with personal information that was potentially impacted. On January 23, 2023, Marquette determined that personal information of one (1) Maryland resident was potentially accessed and/or acquired by an unknown, unauthorized actor as a result of this incident.

The information that could have been subject to unauthorized access and/or acquisition includes name and Social Security number.

Notice to Maryland Resident

On or about February 21, 2023, Marquette provided written notice of this incident to one (1) Maryland resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Marquette moved quickly to investigate and respond to the incident, assess the security of Marquette systems, and identify potentially affected individuals. Marquette is also working to implement additional safeguards and training to its employees. Marquette is providing access to credit monitoring services for one (1) year, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Marquette is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Marquette is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Marquette is providing written notice of this incident to relevant state regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-2297.

Very truly yours,

Michele Veltri of
MULLEN COUGHLIN LLC

MTV/jc2
Enclosure

EXHIBIT A



MARQUETTE MANAGEMENT

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1 (“NOTICE OF” [SECURITY INCIDENT / DATA BREACH])>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Marquette Management Inc. (“Marquette”) writes to inform you of a recent cyber incident that may impact the privacy of some of your information. While we do not have any indication that any identity theft or fraud related to your information has occurred as a result of this incident, this notice provides you with additional information about the incident, our response, and steps you may take to further protect your information against identity theft and fraud, should you determine it is appropriate to do so.

What Happened? On November 30, 2022, Marquette was alerted that an unauthorized party had intercepted email communications between Marquette and a third party. In response, we immediately took steps to secure our email tenant and launched an investigation to determine the nature and scope of the incident. This investigation recently concluded, and determined that between November 4, 2022 and December 1, 2022 an unknown, unauthorized actor gained access to one Marquette email account and potentially accessed and/or acquired certain information stored within that account.

What Information Was Involved? Marquette quickly began a thorough investigation of the relevant emails and files to identify individuals with personal information that was potentially impacted. On January 20, 2023, we determined that your <<b2b_text_2 (“name” and data elements)>><<b2b_text_3 (data elements cont.)>> were potentially accessed and/or acquired by an unknown, unauthorized actor as a result of this incident.

What We Are Doing. Marquette takes this incident and the security of information within our care very seriously. Upon discovery of this incident, we immediately launched an in-depth investigation to determine the full nature and scope of this incident and moved quickly to assess the security of our email accounts and notify potentially affected individuals. As part of our ongoing commitment to the privacy of information within our care, we are working to implement additional security measures to further protect against similar incidents in the future. We will also be notifying state regulators, as required.

As an added precaution, we would like to offer you 12 months of complimentary access to identity monitoring services through Kroll. If you wish to receive these services, you must activate by following the below activation instructions as we are unable to activate these services on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud and to review your accounts statements and credit reports to detect errors or suspicious activity. You can find more information about obtaining a free copy of your credit report, protecting against potential identity theft and fraud, and other resources available to you in the enclosed *Steps You Can Take to Help Protect Your Information*. You may also activate in the complimentary identity monitoring services available to you; detailed instructions for activating these services are enclosed.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, or need assistance, please contact us at (866) 674-3373, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays

Sincerely,

A handwritten signature in black ink, appearing to read 'J. Cunningham', with a stylized flourish extending to the right.

James J. Cunningham
Chief Operating Officer
Marquette Management Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Identity Monitoring Services

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation date)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari, and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Marquette is located at 135 Water St 4th floor, Naperville, IL 60540.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.