Notice of Phishing Incident

Notice of Email Phishing Incident:
Marquette Management - February 7, 2019

What Happened? On October 4, 2018, we became aware of unusual activity relating to an employee's email account. We quickly launched an investigation to determine what may have happened and what information may have been affected. With the assistance of computer forensic experts, our investigation determined that an unknown individual had access to an employee's email account on October 3, 2018 and October 4, 2018 and was later used to send out phishing emails. The investigation was unable to determine which specific emails may have been viewed by the unknown individual. We then undertook a programmatic and manual review of emails that were accessible to identify what personal information was stored within the emails and to whom that information relates. Although we are unaware of any actual or attempted misuses of the personal information, we are providing notice out of an abundance of caution.

What Information Was Involved? Our investigation confirmed the types of information present in the impacted email account included names and Social Security numbers, driver's license numbers, credit/debit card information, financial account information, health insurance information, and medical information.

What Are We Doing. The security of the information provided to us is among our highest priorities. We have strict security measures in place to protect information in our care. Upon learning of this incident, we quickly took steps to confirm the security of our systems, including our employee email accounts. We reset the passwords for all email accounts and reviewed our company policies and procedures relating to data security. In an abundance of caution, we are also notifying individuals and providing access to 12 months of free identity protection services.

What You Can Do? Marquette Management established a dedicated hotline for potentially affected individuals to contact with questions or concerns regarding this incident. For additional information, please call 1-855-904-5765 (toll-free), Monday through Saturday from 8:00 a.m. to 8:00 p.m. CT. Potentially affected individuals may also consider the information and resources outlined below.

Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	TransUnion	Equifax
PO Box 9554	P.O. Box 2000	PO Box 105788

Notice of Phishing Incident

Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will 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.);
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.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 agencies listed below:

Experian	TransUnion	Equifax
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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. This notice has not been delayed by law enforcement.

For North Carolina residents, the North Carolina Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 919-716-6400; and www.ncdoj.gov.