

STATE OF NH
DEPT OF JUSTICE

BakerHostetler

MAY -2 AM 9:28

Baker & Hostetler LLP

999 Third Avenue
Suite 3600
Seattle, WA 98104-4040

T 206.332.1380
F 206.624.7317
www.bakerlaw.com

Randal L. Gainer
direct dial: 206.332.1381
rgainer@bakerlaw.com

April 29, 2016

Via Overnight Mail

Joseph Foster
Office of the Attorney General
33 Capitol St
Concord, NH 03301

Re: Incident Notification

Dear Attorney General Foster:

Our client, the Union League Club of Chicago (“Union League”) understands the importance of the privacy and confidentiality of personal information. On March 5, 2016, Union League learned that one of its employees was using keylogging software on certain Union League computers without authorization. Upon learning of the employee’s use of the software, Union League promptly began an investigation, including retaining an expert computer security firm to examine all Union League computers. On April 7, 2016, Union League determined that the information captured by the keylogger software included payment card information for certain Union League members and guests.

The information the employee may have obtained without authorization included certain member and guest names, payment card numbers, and payment card expiration dates for payment cards used at Union League from December 10, 2015 to March 2, 2016. The employee has been terminated. Union League has notified the Federal Bureau of Investigation of the incident and is cooperating with its investigation.

Beginning on April 29, 2016, Union League is notifying two New Hampshire residents pursuant to New Hampshire law in substantially the same form enclosed with this letter.¹ Union League has also established a dedicated call center to assist individuals with any questions they may have regarding the incident.

¹ As Union League does not conduct business in New Hampshire, this letter is not, and does not constitute, a waiver of personal jurisdiction.

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

Joseph Foster
April 29, 2016
Page 2

In addition to ensuring that this issue is fully remediated, Union League removed the keylogger software and is enhancing its technical safeguards related to employee access to personal information to help prevent something like this from happening in the future.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in blue ink that reads "R. L. Gainer". The signature is written in a cursive style with a large initial "R".

Randal L. Gainer
Partner

Enclosure



UNION LEAGUE CLUB OF CHICAGO

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<mail id>>
<<First Name>> <<Last Name>>
<<Address1>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<First Name>> <<Last Name>>:

The Union League Club of Chicago is committed to protecting the security and confidentiality of the personal information of our members and guests. We are writing to inform you about an incident that may involve some of your information.

On March 5, 2016, we learned that a Union League employee was using keylogging software on certain Union League computers without authorization. Upon learning of the employee's use of the software, we promptly began an investigation, including retaining an expert computer security firm to examine Union League computers. Through the investigation, we determined that the employee used the keylogger software to obtain information entered into certain Union League computers, including payment card information regarding payments made by some of our guests. We determined that the information the employee may have obtained without authorization included your name, payment card number, and payment card expiration date. The employee has been terminated. We have notified the Federal Bureau of Investigation of the incident and are cooperating with its investigation. Based on the investigation, it is possible that payment cards used at Union League from December 10, 2015 to March 2, 2016 may have been affected.

To date, we have no evidence that any of the information copied by the employee has been misused. We are notifying you about this incident so that you can take appropriate steps to protect your information. We recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your account statements for any unauthorized activity. You should immediately report any unauthorized charges to your financial institution because the major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are reported in a timely manner.

We deeply regret any inconvenience this may have caused you. To help prevent something like this from happening in the future, the keylogger software was removed, and we are enhancing our technical safeguards related to employee access to personal information. If you have any questions, please call 1-844-812-9518 Monday through Friday between 8:00 a.m. and 8:00 p.m. Central Time.

Sincerely,

Mark D. Tunney
General Manager

More Information About Ways to Protect Yourself

We encourage you to remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank, and other financial statements for any unauthorized activity. You may also obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit report, free of charge, once every 12 months, please visit www.annualcreditreport.com, or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is as follows:

Equifax
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com
1-800-465-7166

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

TransUnion
P.O. Box 2000
Chester, PA 19022
www.transunion.com
1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov
1-877-438-4338

You can obtain information from these sources about the steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.