

BakerHostetler

RECEIVED
JUL 27 2017
CONSUMER PROTECTION

Baker & Hostetler LLP

2929 Arch Street
Cira Centre, 12th Floor
Philadelphia, PA 19104-2891

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

Erich Falke
direct dial: 215.564.6529
efalke@bakerlaw.com

July 26, 2017

VIA OVERNIGHT MAIL

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

Re: *Incident Notification*

Dear Sir or Madam:

We are writing on behalf of our client, Al J. Schneider Company (“Al J. Schneider”), to notify you of a security incident involving New Hampshire residents at the Galt House Hotel (“Hotel”), an Al J. Schneider hotel.

On June 26, 2017, Al J. Schneider’s investigation determined that malware had been installed on its payment card processing system that copied some Hotel guests’ payment card data, including the cardholders’ names, payment card account numbers, card expiration dates, and verification codes. The investigation determined that payment card data of certain guests who used their cards at the Hotel from December 21, 2016, to April 11, 2017, may have been obtained by an unauthorized person.

On July 26, 2017, Al J. Schneider notified by U.S. mail 6 New Hampshire residents of the incident in substantially the same form as the enclosed letter.¹ For those individuals whom Al J. Schneider does not have a mailing address, Al J. Schneider posted notice of the incident on its website and issued a press release. Additionally, a dedicated call center will be established for affected individuals to call with any questions they may have.

Al J. Schneider has taken measures to contain this incident and eradicate the malware. To help prevent a similar incident from happening in the future, Al J. Schneider continues to further

¹ This report is not, and does not constitute, a waiver of Al J. Schneider’s objection that New Hampshire lacks personal jurisdiction over Al J. Schneider regarding any claims related to the data security incident.

July 26, 2017
Page 2

strengthen the security of its systems including modifying existing two factor authentication for remote access and deploying endpoint threat monitoring tools in the network environment.

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

Sincerely,

A handwritten signature in black ink, appearing to be 'EFA', with a long horizontal stroke extending to the right.

Erich Falke

Enclosure



GALT HOUSE HOTEL

The Heart of Louisville

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Date>> (Format: Month Day, Year)
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Dear <<MemberFirstName>> <<MemberLastName>>,

The Galt House Hotel greatly values the relationship we have with our guests and understands the importance of protecting their payment card information. Regrettably, we are writing to inform you of an incident involving some of that information at our hotel.

After being alerted to a potential information security incident, the Galt House Hotel immediately initiated an investigation of the payment card system that supports card acceptance. In addition to our own internal review, we engaged a leading computer forensics firm to assist us and coordinated closely with law enforcement. On June 26, 2017, our investigation determined that malware had been installed on our payment card processing system that copied some guests' payment card data, including the cardholders' names, payment card account numbers, card expiration dates, and verification codes. The investigation determined that payment card data of certain guests who used their cards at the Galt House Hotel from December 21, 2016, to April 11, 2017, had been obtained by an unauthorized person. You are being notified because you used a payment card ending in <<ClientDef1(####)>> at the Galt House Hotel during this time period.

As a best practice, it is always advisable to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to your payment card issuer because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of your payment card. Please see the section that follows this notice for additional steps you may take to protect your information.

The Galt House Hotel has resolved the issue and we continue to work with the computer forensics firm to further strengthen the security of our systems to help prevent this from happening again. In addition, we are working with the payment card networks so that the banks that issue payment cards can be made aware and initiate heightened monitoring.

The Galt House Hotel deeply regrets any concern this may have caused. If you have any questions, please call 1-???-???-???? from 9:00 a.m. to 6:00 p.m. Eastern time, Monday to Friday.

Sincerely,

Nick Briner
General Manager

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, 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 state. You can obtain information from these sources about 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. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft