

BakerHostetler

RECEIVED

MAR 19 2020

CONSUMER PROTECTION
Baker & Hostetler LLP

811 Main Street
Suite 1100
Houston, TX 77002-6111

T 713.751.1600
F 713.751.1717
www.bakerlaw.com

William R. Daugherty
direct dial: 713.646.1321
wdaugherty@bakerlaw.com

March 13, 2020

VIA FIRST CLASS MAIL

Gordon McDonald
Attorney General
Nebraska Department of Justice
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, BGGMC, LLC (“Benchmark” or “Hotel Contessa”), to notify you of a security incident. Benchmark is a hotel management company that manages Hotel Contessa in San Antonio, Texas.

On February 26, 2020, Hotel Contessa was notified by its third-party reservation services vendor of suspicious login activity on a user’s account for the vendor’s reservation system. Upon learning this, Hotel Contessa immediately took steps to secure the account and launched an investigation. The investigation determined that an unauthorized person accessed the reservation system with the user account at various times between February 18, 2020 and February 26, 2020. Although the investigation was unable to determine which, if any, Hotel Contessa reservations were accessed, the information accessible to the unauthorized person included names, addresses, email addresses, phone numbers, dates of stay, and payment card numbers and expiration dates (but not card verification value, or “CVV”) of some Hotel Contessa guests, including sixteen (16) New Hampshire residents.

On March 13, 2020, Hotel Contessa will begin mailing notification letters via United States Postal Service First Class Mail to the sixteen (16) New Hampshire residents in accordance with

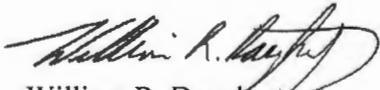
Gordon McDonald
March 13, 2020
Page 2

N.H. Rev. Stat. § 359-C:20.¹ A sample copy of the notification letter is enclosed. Hotel Contessa has established a dedicated call center where all individuals may obtain more information regarding the incident.

To help prevent a similar incident from occurring in the future, Hotel Contessa is continuing to work internally and with its reservation services vendor to evaluate additional security enhancements. In addition, Hotel Contessa reported the incident to law enforcement and is working with the payment card networks so that the banks that issue payment cards can be made aware and initiate heightened monitoring.

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

Sincerely,



William R. Daugherty
Partner

Enclosure

¹ This report is not and does not constitute a waiver of BGGMC's or Hotel Contessa's objection that New Hampshire lacks personal jurisdiction over it related to any claims that may arise from this incident.

Hotel Contessa
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111



March 13, 2020

D-2617

Dear ,

Hotel Contessa values the relationship we have with our guests and understands the importance of protecting payment card information. We are writing to inform you of a security incident that we have identified and addressed that may have involved your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

On February 26, 2020, our third-party reservation services vendor notified us of suspicious login activity on a user's account for the vendor's reservation system. Upon learning this, we immediately took steps to secure the account and launched an investigation. The investigation determined that an unauthorized person accessed the reservation system with the user account at various times between February 18, 2020 and February 26, 2020. Although the investigation was unable to determine which, if any, Hotel Contessa reservations were accessed, the information accessible to the unauthorized person included your name, address, email address, phone number, dates of stay, as well as your payment card number and expiration date (but not card verification value, or "CVV") for your payment card ending in [REDACTED]

While we have no evidence at this time that your information was actually viewed by the unauthorized person, or that it has been misused, it is always advisable to review your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to your 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 following pages for information on additional steps you may take.

To help prevent a similar incident from occurring in the future, we continue to work internally and with our reservation services vendor to evaluate additional security enhancements. In addition, we reported the incident to law enforcement and are working with the payment card networks so that the banks that issue payment cards can be made aware and initiate heightened monitoring.

We regret this incident occurred and apologize for any inconvenience. If you have any questions, please call 1-844-203-4999, Monday through Friday, between 8:30 a.m. and 5:30 p.m. Central Time.

Sincerely,



Troy Mathews, General Manager
BMC – The Benchmark Management Company
Manager, Hotel Contessa

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be 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

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us; Mailing Address: 306 West Market Street, San Antonio, TX 78205

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection/>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island: This incident involves 2 individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below.

For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies 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 reports to be provided to employers.
- You may limit “prescreened” offers of credit and insurance you get based on information in your credit report.
- You have a 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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.