

Sandy B. Garfinkel, Esq.
(412) 566-6868
sgarfinkel@eckertseamans.com

October 24, 2019

VIA FIRST CLASS MAIL

Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

RECEIVED
OCT 28 2019
CONSUMER PROTECTION

Re: Notice of Data Security Incident

To Whom It May Concern:

This notice is provided on behalf of my client, 414 New York LLC (the "Hotel"). As a result of its investigation, the Hotel determined that some of the personal information that it maintained about its guests was accessed without authorization.

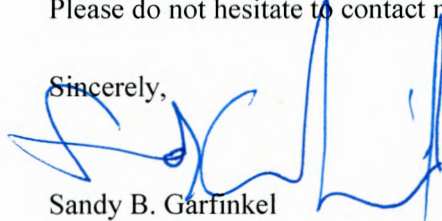
On September 13, 2019, the Hotel learned that an employee who was authorized to access guest credit card information, including credit card numbers, security codes and expiration dates, had done so without authorization. The employee may also have accessed guests' names, dates of stay, and contact information without authorization. Notably, the employee did **not** access guests' Social Security or driver's license numbers. Beginning on May 7, 2019, the employee charged certain guests' credit cards in an amount constituting a portion of their stay and deposited the money in a private account. At no point were guests charged more than what the hotel charge would have otherwise been. The Hotel is absorbing the loss from the fraudulent charges.

Upon learning of the employee's actions, the Hotel immediately terminated the employee's access to the Hotel's system, changed all system passwords, and terminated that individual's employment with the Hotel. The Hotel also reported the incident to local law enforcement and the Federal Bureau of Investigation ("FBI"). In addition, the Hotel is reviewing its privacy policies, limiting employee access to guest information, and retraining its employees appropriately.

The Hotel notified two (2) New Hampshire residents, via U.S. mail, on October 24, 2019. The notice letters included instructions on how to obtain free credit reports and security freezes, along with general advice on how to protect one's identity. A copy of the notice sent to the affected New Hampshire residents is attached.

Please do not hesitate to contact me if you have any questions or concerns.

Sincerely,



Sandy B. Garfinkel

Enclosures



414 W 46TH STREET
NEW YORK, NY 10036

October 24, 2019

NOTICE OF DATA BREACH

Dear _____:

The 414 Hotel (the “Hotel”) is writing to inform you of an incident that may affect the security of your personal information. We take this incident very seriously and are providing you with information and access to resources so that you can better protect against the possibility of misuse of your personal information, should you feel it appropriate to do so.

The privacy and protection of our guests’ information is a matter we take very seriously. We apologize for any concern or inconvenience that may be caused by this incident and we recommend that you closely review this letter for steps that you may take to further protect yourself against any potential misuse of your information.

What Happened

Beginning on May 7, 2019, a Hotel employee, who was authorized to work with the Hotel’s computerized reservations system, accessed reservation information and made unauthorized charges to certain guests’ credit cards. The employee deposited the improperly charged amounts in a private account opened by the employee.

We have not discovered any instance where a card was charged more than what the hotel charge would have otherwise been. The Hotel is absorbing the loss from the fraudulent charges.

Upon learning of the incident on September 13, 2019, the Hotel immediately took action to secure the reservations system from access by that individual and to prevent any further unauthorized charges to guest payment cards. Passwords to the system were changed. The employee was promptly terminated and the matter was reported to local law enforcement and the Federal Bureau of Investigation (“FBI”). Although the Hotel believes that its actions have prevented further potential misuse of its reservations information, out of an abundance of caution, the Hotel is now notifying all potentially affected individuals so that they may take measures to protect themselves from any possible future misuse of the information.

What Information Was Involved

The reservations information to which the employee had access included: Name(s) of guest(s); contact information of guest (address, and in some cases e-mail address); credit card number; expirations dates; security codes; and, dates of stay.

What We Are Doing

As stated above, as soon as it became aware of the unauthorized activity, the Hotel promptly notified local law enforcement authorities and the FBI of the incident. The Hotel changed the passwords required to access its computerized reservations system and terminated the employee. The Hotel is reviewing its privacy policies, limiting employee access to guest information, and will retraining its employees appropriately.

What You Can Do

You should remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports for any unauthorized activity. Information on additional ways to



414 W 46TH STREET
NEW YORK, NY 10036

protect your information, including how to obtain a free credit report and free security freeze, can be found at the end of this letter.

If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions, as major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges if they are reported in a timely fashion. If you believe your credit card information may be compromised, you should consider contacting your credit card company and requesting that the card be reissued with a new printed card security code, replaced with a new card number, or be cancelled. We encourage you to report any suspected unauthorized activity to local law enforcement.

For More Information

We understand that you may have questions about this incident that are not addressed in this letter. We have established a confidential, toll-free hotline to assist you with questions regarding this incident and steps you can take to protect yourself against identity theft and fraud. We apologize for any inconvenience caused by this incident. If you have any questions regarding this incident or if you desire further information or assistance, please contact me toll-free at (866) 987-3280 or by email at admin@414hotel.com.

Sincerely,

/s/ Nick Carmichael
Nick Carmichael, CFO



414 W 46TH STREET
NEW YORK, NY 10036

MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Contact information for the three nationwide credit reporting agencies is:

Equifax, PO Box 105788, Atlanta, GA 30348, www.equifax.com, 1-888-298-0045

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

TransUnion, PO Box 160, Woodlyn, PA 19094, www.transunion.com, 1-888-909-8872

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for 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 agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maryland, Massachusetts, and New Jersey residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You have the ability to place a security freeze on your credit report at no cost to you. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. 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. You may also contact these agencies for information on how to prevent or avoid identity theft through fraud alerts and security freezes.



414 W 46TH STREET
NEW YORK, NY 10036

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

Maryland Residents: For additional information on protection against identity theft, contact the Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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 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 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 a 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. You can 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.

North Carolina Residents: For additional information on protection against identity theft, contact the Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Rhode Island Residents: For additional information on protection against identity theft, contact the Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. You have the right to file and obtain a copy of a police report concerning any fraud or identity theft committed using your personal information.