

**ECKERT
SEAMANS**
ATTORNEYS AT LAW

Eckert Seamans Cherin & Mellott, LLC
U.S. Steel Tower
600 Grant Street, 44th Floor
Pittsburgh, PA 15219

TEL 412 566 6000
FAX 412 566 6099
www.eckertseamans.com

Sandy B. Garfinkel
412.566.6868
sgarfinkel@eckertseamans.com

August 7, 2017

VIA U.S. MAIL

Office of the Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

Re: Data Security Incident Involving Personal Information

To Whom It May Concern:

My firm represents the management company that operates the Hyatt Centric The Loop, Chicago, Illinois (the "Hotel"). I write to inform you an incident involving cyber intrusion and theft of personal information from the Hotel's computer system.

Specifically, guest payment card information for guests who used payment cards at check-in from September 27, 2016 to April 28, 2017 may have been compromised and may have been used for an unauthorized purpose. An unauthorized person installed malware on the Hotel's front desk computer system designed to capture credit and debit card information. The malware captured payment card data intermittently during this time period. Upon learning of the suspicious activity, the Hotel immediately contacted appropriate federal law enforcement officials, initiated an internal review, and engaged a third-party cybersecurity firm that deployed monitoring software at the Hotel. The firm quickly identified the malicious software and removed it from hotel systems. The Hotel also took steps to upgrade security tools protecting the front desk system.

Information that was potentially affected by the malware attack included names printed on customers' credit or debit cards, credit or debit card numbers, card verification codes, and card expiration dates. The Hotel has reported the incident to the U.S. Secret Service and has upgraded the security features of its computer system with software that is capable of identifying and deactivating the malware used in this attack.

Due to the unusual nature of the new type of malware used in this attack, the forensic investigation and identification of affected individuals was more difficult and time consuming than anticipated. These items were just completed within the past several days. The Hotel is

RECEIVED

AUG 10 2017

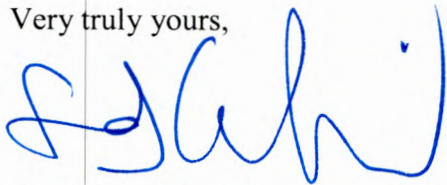
CONSUMER PROTECTION

**ECKERT
SEAMANS**
ATTORNEYS AT LAW

preparing to send notification letters to potentially affected individuals, including 8 residents of New Hampshire. A copy of the notification letter is attached. The notification letters will be sent on approximately August 7, 2017. In addition to the letters, the Hotel has provided substitute notification nationwide via website posting because some contact information for affected guests was not able to be ascertained, which was posted on August 4, 2017. The Hotel is also providing, at its sole cost, the option for each potentially affected guest to enroll in a credit monitoring protection program for one (1) year, furnished through a nationally recognized identity theft vendor.

If you have any further questions about the incident, do not hesitate to contact me.

Very truly yours,



Sandy B. Garfinkel

Enclosures

Integrated Clark Monroe, LLC

181 W. Madison St.
Suite 4700
Chicago, IL 60602

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

**Important Security Notification -
Please read this entire letter**

Re: Hyatt Centric The Loop Chicago

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

This letter is to inform you of a data security incident at the Hyatt Centric The Loop Chicago (the "Hotel") that may affect you. Integrated Clark Monroe, LLC is the owner of the Hotel.

An unauthorized person installed malware on the Hotel's front desk computer system designed to capture credit and debit card information. Specifically, guest payment card information for guests who used payment cards at check-in from September 27, 2016 to April 28, 2017 may have been compromised and may have been used for an unauthorized purpose.

NOTE: This Security Incident does not involve Hyatt's or Interstate Management Company's systems. This incident only involves the front desk computer system of this franchised hotel.

Upon learning of the suspicious activity, the Hotel immediately contacted appropriate federal law enforcement officials, initiated an internal review, and engaged a third-party cybersecurity firm that deployed monitoring software at the Hotel. The firm quickly identified the malicious software and removed it from Hotel systems. The Hotel also took steps to upgrade security tools protecting the front desk system.

Information that was potentially affected by the malware includes names printed on customers' credit or debit cards, credit or debit card numbers, card verification codes, and card expiration dates. The Hotel has reported the incident to the proper authorities and as a result of this incident, the Hotel has upgraded the security features of its computer system with software that is capable of identifying and deactivating the malware used in this attack.

Integrated Clark Monroe, LLC, as the owner of the Hotel, is providing you with this notification letter so that you may be on guard for any signs of unauthorized use of your credit card information. You are urged to be vigilant for signs of fraudulent activity by reviewing your credit card account statements regularly and obtaining and reviewing your free credit report concerning your credit activity. There are instructions for obtaining your free credit report in the attached pages. If you suspect that fraudulent activity has occurred, you should report it to your local law enforcement agency, to your state's attorney general's office and/or to the U.S. Federal Trade Commission ("FTC") (contact information for the FTC is provided in the attached pages).

It is unlikely that credit card information alone could be used in a way that would adversely impact your credit. However, out of an abundance of caution, as described in more detail below, the Hotel will be providing further services for one year at no cost to you via a credit monitoring program furnished through a nationally recognized vendor, Kroll Information Assurance, LLC. Additional information about the credit monitoring program and enrollment in the program can be accessed at www.loopchicagohotel.com. To receive services by mail instead of online, please call 855-205-6943. Please note that Kroll's activation website is only compatible with the current version or one earlier of Internet Explorer, Chrome, Firefox and Safari. To receive the services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name and have a U.S. residential address associated with your credit file.

Please note when these types of incidents occur, some criminals seek to fraudulently obtain the personal information of affected individuals by claiming to be the business that experienced the incident. We advise you NOT to respond to any requests from entities requesting your sensitive personal information in relation to this incident. Neither the Hotel nor anyone legitimately contacting you on its behalf will ask you for other sensitive personal information with regard to this incident. You will only be asked for the most limited amount of information necessary to provide the identity protection services.

Guests who suspect unauthorized activity should report it to the issuer of the credit or debit card. The policies of the payment card brands such as Visa, MasterCard, American Express and Discover provide that you have zero liability for any unauthorized charges if you report them in a timely manner.

We deeply regret and apologize that this incident has occurred and reaffirm our commitment to protect the personal information of our guests. If you have questions regarding this situation and the actions you can take to protect yourself, or the complimentary credit monitoring services, please call our dedicated Call Center at 855-205-6943, or Neil Grammer, Interstate Management Company, LLC, at (703) 387-3327.

Sincerely,

A handwritten signature in cursive script, appearing to read "Karen McGuigan".

Karen McGuigan
General Manager
Hyatt Centric The Loop Chicago

ADDITIONAL RESOURCES, CREDIT ALERTS AND FREEZES

Information about Identity Theft

Federal Trade Commission

The Federal Trade Commission provides helpful information about how to avoid identity theft.

- Visit: <http://www.ftc.gov/idtheft>
- Call (toll-free): 1-877-ID-THEFT (1-877-438-4338)
- Write: Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., NW, Washington, DC 20580
- It is recommended that you report suspected identity theft to law enforcement, including the Federal Trade Commission

Free Annual Credit Reports

You may obtain a free copy of your credit report once every 12 months.

- Visit: <http://www.annualcreditreport.com>
- Call (toll-free): 1-877-322-8228
- Write: Complete an Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281 (you can print a copy of the form at <http://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf>).

You also may purchase a copy of your credit report by contacting one of the three national credit reporting companies.

Equifax

1-800-525-6285
www.equifax.com
P. O. Box 740241
Atlanta, GA 30374-0241

Experian

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

TransUnion

1-800-888-4213
www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19022

Fraud Alerts: "Initial Alert" and "Extended Alert"

You can place two types of fraud alerts 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." An Initial Alert stays on your credit report for 90 days. You may ask that an Initial Alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An Extended Alert stays on your credit report for seven years. To obtain the Extended Alert, you must provide proof to the credit reporting company (usually in the form of a police report) that you actually have been a victim of identity theft. You have the right to obtain a police report regarding the data security incident. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three credit reporting companies provided above.

A potential drawback to activating a fraud alert would occur when you attempt to open a new account. You would need to be available at either your work phone number or home phone number in order to approve opening the new credit account. If you are not available at either of those numbers, the creditor may not open the account. In addition, it may take longer to obtain credit and in some cases merchants may be hesitant to open a new account.

Fraud alerts will not necessarily prevent someone else from opening an account in your name. A creditor is not required by law to contact you if you have a fraud alert in place. Fraud alerts can legally be ignored by creditors. If you suspect that you are or have already been a victim of identity theft, fraud alerts are only a small part of protecting your credit. You also need to pay close attention to your credit report to make sure that the only credit inquiries or new credit accounts in your file are yours.

You may contact all of the three major credit reporting agencies using the information below that they have published. Credit agencies will need to verify your identity which will require providing your Social Security number and other similar information.

TransUnion

P.O. Box 2000
Chester, PA 19022-2000
<https://fraud.transunion.com>
1-800-680-7289

Equifax

P. O. Box 740241
Atlanta, GA 30374-0241
https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp
1-888-766-0008

Experian

P. O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
1-888-397-3742

Placing a fraud alert does not damage your credit or credit score. Additional information may be obtained from www.annualcreditreport.com.

If you are a resident of **Maryland**, you may contact the Maryland Attorney General's Office at 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

If you are a resident of **North Carolina**, you may contact the North Carolina Attorney General's Office at 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400 or toll free at 1-877-566-7226.

If you are a resident of **Rhode Island**, you may contact the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, <http://www.riag.ri.gov>.

If you are a resident of **Iowa**, you may contact law enforcement or Iowa Office of the Attorney General: Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, 515-281-5164, www.iowaattorneygeneral.gov.

If you are a resident of **Oregon**, you may contact the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, 503-378-4400, <http://www.doj.state.or.us>.

If you are a resident of **New Mexico**, you have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov.

Credit or Security Freeze on Credit File

All consumers may also place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, mortgages, employment, housing or other services.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent; however, using a security freeze may interfere with or delay your ability to obtain credit. To place a security freeze on your credit report, contact the credit reporting agencies using the information below, and be prepared to provide the following (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 two 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. The consumer reporting agency may charge a fee of between \$5.00 and \$20.00 to place, lift, and/or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and you

have submitted a valid police report relating to the identity theft incident to the consumer reporting agency. The addresses of consumer reporting agencies to which requests for a security freeze may be sent are:

TransUnion

P.O. Box 2000
Chester, PA 19022-2000
<https://freeze.transunion.com>

Equifax

Equifax Security Freeze
P.O. Box 105788
Atlanta, Georgia 30348
[https://www.freeze.equifax.com/
Freeze/jsp/SFF_PersonalIDInfo.jsp](https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp)

Experian

P. O. Box 9532
Allen, TX 75013
[https://www.experian.com/
freeze/center.html](https://www.experian.com/freeze/center.html)

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include:

- proper identification (name, address, and Social Security number);
- the PIN or password provided to you when you placed the security freeze; and
- the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available.

The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.