



MULLEN  
COUGHLIN<sub>LLC</sub>  
ATTORNEYS AT LAW

RECEIVED  
MAY 29 2019  
CONSUMER PROTECTION

Edward J. Finn  
Office: 267-930-4776  
Fax: 267-930-4771  
Email: [efinn@mullen.law](mailto:efinn@mullen.law)

1275 Drummers Lane, Suite 302  
Wayne, PA 19087

May 24, 2019

**VIA U.S. MAIL**

Attorney General Gordon J. MacDonald  
Office of the New Hampshire Attorney General  
Consumer Protection Bureau  
33 Capitol Street  
Concord, NH 03301

**Re: Notice of Data Security Incident**

Dear Attorney General Gordon J. MacDonald:

We represent HP Restaurant Group (“Hyde Park”) headquartered at 21945 Chagrin Blvd, Beachwood, OH 44122 and are writing to provide notice to your office of an incident that may affect the security of credit and debit card information relating to certain New Hampshire residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Hyde Park does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data incident notification statute, or personal jurisdiction.

**Nature of the Data Event**

On or about April 5, 2019, Hyde Park was notified of suspicious activity regarding its online payment processing platform. Hyde Park immediately launched an investigation with the assistance of a third-party forensic firm to determine the nature and scope of the activity. On or about April 29, 2019, the forensic investigation determined it was possible that customer credit and debit card information for transactions that occurred on Hyde Park’s e-commerce gift card website since 2011 may have been subject to unauthorized access and/or acquisition. Hyde Park provided notice to individuals whose credit and debit cards were used on their e-commerce gift card website during the relevant period. This incident only affected transactions made on Hyde Park’s e-commerce gift card website. No transactions made in Hyde Park’s restaurants were affected.

Attorney General Gordon J. MacDonald

May 24, 2019

Page 2

The information that could have been subject to unauthorized access includes customer names, credit or debit card numbers, card expiration date, and card security number or CVV. Certain customers' Hyde Park user account names and passwords may also have been affected.

### **Notice to New Hampshire Residents**

On or about May 24, 2019, Hyde Park provided written notice of this incident to all potentially affected individuals, which includes forty-two (42) New Hampshire residents, which includes all individuals who used a card during the window of compromise and whose information may have been exposed. Written notice is being provided in substantially the same form as the letter attached hereto as *Exhibit A*.

### **Other Steps Taken and To Be Taken**

Upon discovering the event, Hyde Park moved quickly to investigate the incident, minimize risk to the information, and to provide the affected individuals with notice of this incident. Hyde Park immediately shut down the affected website and moved its online gift card processing to a completely new environment.

Additionally, Hyde Park is providing all impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Hyde Park is also providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Hyde Park has reported this incident to the credit card companies. Hyde Park is also providing written notice of this incident to other state regulators and the consumer reporting agencies, as required.

### **Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4776.

Very truly yours,



Edward J. Finn of  
MULLEN COUGHLIN LLC

# EXHIBIT A



<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>  
<<Address1>>  
<<Address2>>  
<<City>>, <<State>> <<Zip>>

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

HP Restaurant Group ("Hyde Park") is writing to inform you about an incident that occurred possibly compromising the security of your credit or debit card information. Hyde Park recently discovered that customer credit and debit card data that was entered into the e-commerce gift card website may have been captured by unauthorized actors. We can assure you this incident did not affect any card transactions at our restaurant locations. The incident affected only the e-commerce gift card website, and not any of the Hyde Park restaurant locations. We take this incident very seriously and are providing you with information and access to resources so that you can protect your personal information, should you feel it is appropriate to do so.

**What Happened?** On or about April 5, 2019, Hyde Park was notified of suspicious activity regarding our online payment processing platform. Hyde Park immediately launched an investigation with the assistance of a third-party forensic firm to determine the nature and scope of the activity. On or about April 29, 2019, the forensic investigation determined it was possible that customer credit and debit card information for transactions that occurred on Hyde Park's e-commerce gift card website since 2011 may have been subject to unauthorized access and/or acquisition. While the investigation was unable to definitively confirm whether your card data was accessed or taken, Hyde Park is notifying you in an abundance of caution because we have confirmed that your credit or debit card was used for a transaction on our website during the relevant time-period, and your information may be affected.

**What Information Was Involved?** The information potentially affected includes your name and address, credit or debit card number, expiration date, and card security code number or CVV. Your Hyde Park account username and password may also have been affected.

**What We Are Doing.** We take the security of information in our care very seriously. We have security measures in place to help protect the data on our systems and are working to implement additional safeguards to further protect the privacy and security of information in our care. We immediately shut down the affected website and moved our online gift card processing to a completely new environment. This incident has been reported to your credit card company, and we will be reporting this incident to certain state regulators and Attorneys General.

**What You Can Do.** Please review the enclosed "Steps You Can Take to Prevent Identity Theft and Fraud." We advise you to report any suspected incidents of identity theft to your credit card company and/or bank. If you have a Hyde Park online account, you should promptly change your password, security question and/or answer, and take appropriate steps to protect any other online accounts that have the same user name or email address and password, security question, and/or answer.

**For More Information.** We understand that you may have questions about this incident that are not addressed in this letter. Inasmuch as this incident did not occur at any of the restaurant locations, the employees have no information and are not able to answer inquiries or provide any explanation. Accordingly, we kindly request that all inquiries be directed to the call center which has been set up for dedicated assistance. You may reach them at 800-490-8715, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time.

Hyde Park takes the privacy and security of the information in our care seriously. We regret any concern this situation has caused you. Once again, we assure you this incident did not affect any gift card purchases or in store transactions at our restaurant locations.

Sincerely,

A handwritten signature in black ink that reads "Robert T. Gaglione". The signature is written in a cursive style with a large, prominent initial "R".

Robert T. Gaglione  
Chief Financial Officer

## STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

We advise you to remain vigilant by reviewing all account statements and monitoring free credit reports.

### **Monitor Your Accounts.**

**Credit Reports.** We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the major credit reporting bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the major credit bureaus listed below to request a free copy of your credit report.

**Fraud Alerts.** At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

**Security Freeze.** You have the 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. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

#### **Experian**

PO Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

#### **TransUnion**

P.O. Box 2000  
Chester, PA 19016  
1-888-909-8872  
[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

#### **Equifax**

PO Box 105788  
Atlanta, GA 30348-5788  
1-800-685-1111  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

In order to request a security freeze, you will need to supply the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

**Additional Information.** You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice has not been delayed as a result of a law enforcement investigation.

**For Maryland residents**, the Attorney General can be contacted by mail at 200 St. Paul Place, Baltimore, MD, 21202; toll-free at 1-888-743-0023; by phone at (410) 576-6300; consumer hotline (410) 528-8662; and online at [www.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov). **For 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 violators. 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://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. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should also be reported to law enforcement. **For North Carolina Residents:** The North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400, and online at [www.ncdoj.gov](http://www.ncdoj.gov). **For Rhode Island Residents:** The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are approximately twenty (20) Rhode Island residents impacted by this incident.