NELSON MULLINS

NELSON MULLINS RILEY & SCARBOROUGH LLP
ATTORNEYS AND COUNSELORS AT LAW

Atlantic Station
201 17th Street, NW | Suite 1700
Atlanta, GA 30363
T 404.322.6000 F 404.322.6050
nelsonmullins.com

David F. Katz
T 404.322.6122
david.katz@nelsonmullins.com

January 31, 2019

VIA FedEx

Wayne Stenehjem
North Dakota Attorney General
600 E. Boulevard Avenue, Dept. 125
Bismarck, ND 58505

RE: Data Security Incident Notification

Dear Attorney General:

I am writing to inform you of a data security incident that may affect 250 or more North Dakota residents. Our client, Huddle House, Inc. will publish the attached substitute notification on its website on February 1, 2019, and provide notice to statewide media.

On January 3, 2019, Huddle House learned that various locations were recently the target of malicious cyber activity involving some corporate and franchisee operated restaurants. Criminals compromised a third-party point of sale (POS) vendor's data system and utilized the vendor's assistance tools to gain remote access—and the ability to deploy malware—to some Huddle House corporate and franchisee POS systems. In less than 24 hours from learning of the intrusion, Huddle House engaged a leading IT investigation and security firm to determine the facts and contain the intrusion and commenced remediation procedures. Its investigation found that an intruder placed malware into the POS system at some corporate and franchise locations, and by doing so gained unauthorized access to certain payment card information from the magnetic stripe, including cardholder name, credit/debit card number, expiration date, cardholder verification value, and service code. Personal information belonging to consumers who used a payment card at some corporate and franchise locations between August 1, 2017 and present, may be at risk.

Huddle House is unable to determine contact information for each consumer whose information may be at risk. Therefore, it is publishing a substitute notification to its customers on its website, and providing notice to statewide media.

Please let me know if you have any additional questions regarding the notification.

Sincerely,

David F. Katz

Enclosure: Substitute Notice

IMPORTANT SECURITY AND PERSONAL DATA PROTECTION NOTIFICATION

February 1, 2019

Huddle House values the relationship we have with our guests and wants you to be aware of an incident that may involve your payment card. We recently became aware of a malware intrusion that affected some point of sale systems at certain corporate and franchised locations. Promptly after discovering the issue, we immediately engaged a leading IT investigation and security firm to determine the facts. Protecting the security of our customers' personal information is a top priority for Huddle House, Inc., and all of our franchisees. We value and respect the privacy of your information, and we sincerely apologize for any concern or inconvenience this may cause you.

What Happened?

Huddle House locations were recently the target of malicious cyber activity involving some corporate and franchisee operated restaurants. Criminals compromised a third-party point of sale (POS) vendor's data system and utilized the vendor's assistance tools to gain remote access—and the ability to deploy malware—to some Huddle House corporate and franchisee POS systems. Huddle House was notified by a law enforcement agency and its credit card processor that some of its corporate and franchise locations may have been victims of a malicious cyber-attack. Huddle House retained a leading IT investigation and security firm in less than 24 hours from notification, to deploy specialized software to prevent further attacks. At this time, we do not know how many locations may have been infected with malware. If you used a payment card at a Huddle House location between August 1, 2017 and present, your payment card information may be at risk. This date range is based upon our preliminary investigation and we are still conducting our investigation into the scope of this attack. We wanted to alert you of these facts so you can make informed choices about your use of your credit or debit card accounts and how best to protect yourself from potential fraud associated with the unauthorized use of your credit or debit card. You may review the list of all current corporate and franchisee restaurants at this link: https://locations.huddlehouse.com

What Information Was Involved?

Based on the facts known to Huddle House at this time, the malware was designed to collect certain payment card information from the magnetic stripe, including cardholder name, credit/debit card number, expiration date, cardholder verification value, and service code.

What Are We Doing?

In less than 24 hours from learning of the intrusion, we engaged a leading IT investigation and security firm to determine the facts and contain the intrusion and commenced remediation procedures. We have deployed additional IT security measures to reduce risk of further attacks. Huddle House has worked aggressively with third-party forensic experts and federal law enforcement on this investigation, which is ongoing.

How Does This Incident Affect Me?

Even if you used your payment card at one of the locations involved, it does not mean you will be affected by this issue. Out of an abundance of caution, you may want to review and monitor your payment card statements if you used a payment card at an affected location during the referenced dates. If you believe your payment card may have been affected, please contact your bank or card issuer immediately.

What Else Can I Do to Protect My Information?

We recommend that you remain vigilant, review your relevant account statements, and monitor your credit reports for suspicious activity. Some state laws advise you to report any suspected identity theft to law enforcement, your state's Attorney General, and the Federal Trade Commission. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report:

Equifax	**Experian**	**TransUnion**
Phone: 1-800-685-1111 P.O. Box 740241 Atlanta, Georgia 30348 www.equifax.com (//www.equifax.com)	Phone: 888-397-3742 P.O. Box 9532 Allen, Texas 75013 www.experian.com (//www.experian.com)	Phone: 800-680-7289 P.O. Box 6790 Fullerton, CA 92834 www.transunion.com (//www.transunion.com)

For Georgia and Maryland 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 additional report(s).

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. This can be done by contacting the credit bureaus by phone and also via Experian's or Equifax's website. Once you place a fraud alert at one credit bureau, that bureau is required to notify the other two and have alerts placed on your behalf. Note, however, that because the alert tells creditors to follow certain procedures to protect you, it may also delay your efforts to obtain credit while the agency verifies your identity.

Security Freezes: You have the right to place a security freeze on your credit report. A security freeze is intended to prohibit 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, credit mortgages, employment, housing or other services. To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail in order for the freeze to be effective. In order to request a security freeze, you will need to provide the following information: (1) full name (including middle initial and any suffixes); (2) social security number; (3) date of birth; (4) current address and previous addresses for the past five years; (5) proof of current address, such as a current utility bill, bank statement, or insurance statement; (6) a legible photocopy of a government issued identification card (state driver's license, military identification, etc.); (7) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze.

You may also place a security freeze on your credit report online by visiting the below links:
https://www.experian.com/freeze/center.html
https://www.transunion.com/credit-freeze
https://www.equifax.com/personal/credit-report-services/

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit www.identitytheft.gov or call 1-877-ID-THEFT (877-438-4338). IdentityTheft.gov is the federal government's one-stop resource for identity theft victims. The site provides streamlined checklists and sample letters to guide you through the recovery process.

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202 www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Attorney General at http://www.ncdoj.gov, Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 or by calling 1-877-566-7226.

For Illinois residents: If you have been the victim of identity theft or believe your personal or financial information may have been compromised, please call the toll-free Identity Theft Hotline at: 1-866-999-5630 or 1-877-844-5461 (TTY).
http://illinoisattorneygeneral.gov/consumers/hotline.html

Consumer FAQs can be found here [insert hyperlink].