SheppardMullin

Sheppard, Mullin, Richter & Hampton LLP
30 Rockefeller Plaza
New York, New York 10112-0015
212.653.8700 main
212.653.8701 fax
www.sheppardmullin.com

KRollins@sheppardmullin.com

October 5, 2017

VIA ELECTRONIC MAIL

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
consumer@iowa.gov

Re: Notice of Data Breach

Dear Sir or Madam:

We are writing on behalf of our client, SONIC Corp., to inform you that credit and debit card numbers may have been acquired without authorization as part of a malware attack experienced at certain Sonic Drive-In locations.

On September 18, 2017, Sonic was notified by its credit card processor of suspicious activity involving customer credit or debit cards potentially used at Sonic Drive-In locations. Upon learning of the suspicious activity, Sonic immediately notified law enforcement and initiated an investigation into the matter. Law enforcement initially asked Sonic to delay notification. Since learning of this matter, Sonic has been working with experienced forensic investigators and law enforcement to investigate the nature and extent of the criminal activity. These investigations remain ongoing.

Sonic's forensic investigations have revealed that malware may have been used to acquire customer credit or debit card numbers from Sonic's systems without authorization. Sonic publicly informed consumers of the criminal activity on October 4, 2017 via a national press release, advertisement in certain local media, and a public announcement on its website at https://www.sonicdrivein.com/notice-of-data-breach. A copy of the press release is attached. We are also writing to keep you informed of this matter, as we and our client are committed to working with you to address any questions you might have.

Further, as a precautionary measure, Sonic is offering two years of free credit monitoring and theft protection services to any consumer who used a credit or debit card at Sonic Drive-Ins this year. Sonic has also provided consumers with detailed information regarding steps they can take to protect themselves from fraud.

We assure you that our client, Sonic, takes this issue, and the privacy and security of its customers, very seriously and is working diligently to continue to investigate this matter. If you have any questions or require further information, please feel free to contact me at krollins@sheppardmullin.com or (212) 634-3077.

Sincerely,

Kari M. Rollins

Enclosure

Sonic Drive-In: Notice of Payment Card Breach

What Happened
Sonic Drive-In has discovered that credit and debit card numbers may have been acquired without authorization as part of a malware attack experienced at certain Sonic Drive-In locations. Your trust in Sonic is important to us and we sincerely regret any inconvenience this may cause. We have provided here more information about this situation, including an offer of free identity theft protection for affected customers:

What Information Was Involved
Based on our investigations to-date it appears that credit and debit card numbers used at certain Sonic Drive-In locations may have been impacted.

What We Are Doing
Upon learning of this matter we immediately contacted law enforcement and have been working with them in their investigation. We also immediately began our own investigation with the help of experienced third-party forensics firms. Notice of this incident was briefly delayed to accommodate law enforcement's investigation. We regret that this incident occurred, and apologize for any inconvenience or concern it may cause. As a precautionary measure, we are offering customers who used their cards at our locations this year to receive 24 months of free fraud detection and identity theft protection through Experian's IdentityWorks program. To take advantage of these free services, you can enroll by visiting the Experian IdentityWorks website: http://www.experianidworks.com/sonic. You have until **December 31, 2017** to register and enroll. If you have questions or need an alternative to enrolling online, please call 877-534-7032.

What You Can Do
Whenever there is an issue involving credit or debit card numbers, you can always check your statements. You can also monitor your financial accounts and get free credit reports for any incidents of fraud or identity theft. If you see any unauthorized activity, contact your financial institution. You can also report suspected incidents of identity theft to local law enforcement, the Federal Trade Commission ("FTC"), at 1-877-ID-THEFT (1-877-438-4338), or your state Attorney General. In Maryland, you can reach the State Attorney General's office by phone at (888) 743-0023. Its website is http://www.oag.state.md.us/. In North Carolina, you can reach the State Attorney General's office by phone at (919) 716-6400. Its website is http://www.ncdoj.gov. Their mailing addresses are:

Douglas F. Gansler
Attorney General of the State of Maryland
Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

Roy A. Cooper
Attorney General of the State of North Carolina
Consumer Protection Division, Attorney General's Office
Mail Service Center 9001
Raleigh, NC 27699-9001

Additionally, if you believe your identity has been stolen or used without your permission, contact your local police department to file a report.

Fraud alerts: You can place a fraud alert on your bank accounts and credit file as a precautionary step. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus listed below. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. All three credit reports will be sent to you, free of charge, for your review.

- TransUnion, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016 (800) 680-7289 www.transunion.com
- Experian, P.O. Box 9532, Allen, TX 75013 (888) 397-3742 www.experian.com

- Equifax, P.O. Box 740241, Atlanta, Georgia 30374-0241 (800) 525-6285 www.equifax.com

Credit/security freeze: If you believe that your identity has been stolen, consider placing a credit/security freeze on your credit report. Placing a freeze on your credit report will prevent lenders and others from accessing your credit reports in response to a new credit application. With a freeze in place, even you will need to take special steps when you wish to apply for any type of credit. You will need to place a credit freeze separately with each of the three major credit reporting companies if you want the freeze on all of your credit files. A freeze remains on your credit file until you remove it or choose to lift it temporarily when applying for credit. There may be a fee for this service based on state law.

For additional information, and pricing details, visit the credit bureaus at:

TransUnion	https://www.transunion.com/credit-freeze/place-credit-freeze
Experian	https://www.experian.com/blogs/ask-experian
Equifax	https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp

Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.annualcreditreport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

If you have any questions please call us at 877-534-7032.