You are receiving this letter as a current or former employee of Carisch, Inc., which operates Arby's franchises throughout the United States. We respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that may involve your personal information.

On February 14, 2021 Carisch suffered a ransomware attack, which resulted in the attacker's encryption of several network servers and Carisch's inability to access those servers. We detected the incident immediately and took action to disconnect the servers from internet access in an effort to prevent the attackers from taking data from our systems. Due to the nature of ransomware attacks and the quickness of our response, we have no reason to believe any data was stolen or accessed, but, out of an abundance of caution, we are sending these letters to inform you that the impacted systems may have contained your W2 and related employment information. The specific personal information accessed may have included your name, address, and Social Security Number. To our knowledge, the data accessed did NOT include any payroll, banking, or credit card information.

Carisch values your privacy and deeply regrets that this incident occurred. Carisch has completed a thorough review of the impacted systems, but we will notify you if there are any other developments. In addition, at the time of the incident, Carisch was in the process of upgrading our network environment. Due to this network upgrade, we are no longer using any systems or hardware impacted by the security incident and are installing new computers on an entirely new network. Carisch set up its new systems using industry best practices, advanced security features, and the latest operating system and software.

In addition to the above information, you may wish to take the following steps to further protect your information:

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

We recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission

- **Copy of Credit Report**

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. While you do not need it to obtain a copy of your credit report, for your reference, the contact information for the three national credit reporting can be found at the following websites:

- Equifax: www.equifax.com
- Experian: www.experian.com
- TransUnion: www.transunion.com

- **Fraud Alert**

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will state on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

- **Security Freeze**

In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

- **Additional Free Resources on Identity Theft**

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit http://www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). A copy of Identity Theft: A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm.

Carisch takes this matter very seriously and is committed to protecting the privacy and security of all personal information. We are reinforcing our existing policies and practices and evaluating additional safeguards to help prevent a similar incident from occurring in the future. We regret any inconvenience or concern caused by this incident. For further information and assistance, please contact disclosure@carischinc.com.

Sincerely,

Mark Gregory
CFO