29135

March 2, 2023

Dear Valued Chick-fil-A Customer:

In addition to previous communications you may have received from us, Chick-fil-A, Inc. ("Chick-fil-A") is writing to provide you with additional detail of a data security incident that occurred and may have involved your personal information. This notice provides information about the incident, measures we have taken in response, and resources available to you.

What Happened?

We recently identified suspicious login activity to certain Chick-fil-A One accounts. Upon discovery of this activity, which occurred between December 18, 2022 and February 12, 2023, Chick-fil-A immediately took steps to prevent any further unauthorized activity, began an investigation, and engaged a national forensics firm. Based on our investigation, we determined on February 12, 2023 that the unauthorized parties accessed information in your Chick-fil-A One account.

What Information Was Involved?

This information may have included your name, email address, Chick-fil-A One membership number and mobile pay number, QR code, masked credit/debit card number, and the amount of Chick-fil-A credit (e.g., e-gift card balance) on your account (if any). In addition, if saved to your account, the information may have included the month and day of your birthday, phone number, and address. Importantly, unauthorized parties would only have been able to view the last four digits of your payment card number.

What We Are Doing.

Chick-fil-A takes the protection of personal information seriously. As soon as Chick-fil-A discovered the incident, we immediately took action to protect customers' accounts, which included requiring customers to reset passwords, removing any stored credit/debit card payment methods, and temporarily freezing funds previously loaded onto customers' Chick-fil-A One accounts. We also restored customers' Chick-fil-A One account balances, which may have included a refund to your original form of payment, where possible. As an additional way to say thank you for being a loyal Chick-fil-A customer, we have added rewards to your account. Chick-fil-A continues to enhance its security, monitoring, and fraud controls as appropriate to minimize the risk of any similar incident in the future.

What You Can Do.

If you have not done so already, please use the following link to reset your Chick-fil-A password as soon as possible: "How do I reset my password." We urge you to choose a strong password (not easy-to-guess) and unique to Chick-fil-A (e.g., not a password that you use on other websites/accounts).

The enclosed Reference Guide includes additional information on general steps you can take to monitor and protect your personal information. We encourage you to remain vigilant against potential identity theft and fraud by carefully reviewing credit reports and account statements to ensure that all activity is valid.

For More Information.

If you have any questions about this matter or would like additional information, please refer to the enclosed Reference Guide or call toll-free (833) 753-4428. This call center is open from Monday through Friday from 9 am - 9 pm Eastern Time.

We regret that this incident occurred and apologize for any inconvenience it may cause you.

Thank you,

Your Team at Chick-fil-A

Reference Guide

Review Your Account Statements

Carefully review account statements and credit reports to ensure that all of your account activity is valid. Report any questionable charges promptly to the financial institution or company with which the account is maintained.

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a

notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, GA 30348	1-888-766-0008	www.equifax.com
Experian	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	1-800-916-8800	www.transunion.com

Security Freezes

You have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (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 five 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.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	1-800-685-1111	www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	1-888-909-8872	www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

For Residents of Massachusetts

You have the right to obtain a police report with respect to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.