RECEIVED

MAR 02 2023

CONSUMER PROTECTION

ALSTON & BIRD

The Atlantic Building
950 F Street, NW
Washington, DC 20004-1404
202-239-3300 | Fax: 202-239-3333

March 1, 2023

CONFIDENTIAL
VIA OVERNIGHT DELIVERY

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

Re: Notice of Data Security Incident

To the Office of the New Hampshire Attorney General:

We are writing on behalf of Chick-fil-A, Inc. ("Chick-fil-A") to notify you of a data security incident. A copy of the notification being sent to 82 affected New Hampshire residents on March 2, 2023 via e-mail in accordance with notification requirements under state law is attached to this letter.

Chick-fil-A recently identified suspicious login activity to certain Chick-fil-A One accounts. Upon discovery of this activity, Chick-fil-A immediately took steps to prevent any further unauthorized activity, began an investigation, and engaged a national forensics firm. Following a careful investigation, Chick-fil-A determined that unauthorized parties launched an automated attack against its website and mobile application between December 18, 2022 and February 12, 2023 using account credentials (e.g., email addresses and passwords) obtained from a third-party source. Based on Chick-fil-A's investigation, Chick-fil-A determined on February 12, 2023 that the unauthorized parties subsequently accessed information in customers' Chick-fil-A One accounts.

This information may have included a customer's

).

Chick-fil-A takes the protection of personal information seriously. As soon as Chick-fil-A discovered the incident, it 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. Chick-fil-A also restored customers' Chick-fil-A One account balances, which may have included a refund to the customer's original form of payment, where possible. As an additional way to say thank you for being loyal Chick-fil-A customers, Chick-fil-A has added rewards to affected customers' accounts. 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.

If you have any questions regarding this incident or if you desire further information or assistance, please email me at

Sincerely,

Kimberly Peretti

Enclosure

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, Chick-fil-A immediately took steps to prevent any further unauthorized activity, began an investigation, and engaged a national forensics firm. Following a careful investigation, we determined that unauthorized parties launched an automated attack against our website and mobile application between December 18, 2022 and February 12, 2023 using account credentials (e.g., email addresses and passwords) obtained from a third-party source. Based on our investigation, we determined on February 12, 2023 that the unauthorized parties subsequently accessed information in your Chick-fil-A One account.

What Information Was Involved?

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 . 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 the District of Columbia

You may contact the D.C. Attorney General's Office to obtain information about steps to take to avoid identity theft:

D.C. Attorney General's Office, Office of Consumer Protection, 400 6th Street, NW, Washington DC 20001, 1-202-442-9828, www.oag.dc.gov.

For Residents of Iowa

You may contact law enforcement or the Iowa Attorney General's office to report suspected incidents of identity theft. The Iowa Attorney General's Office can be reached at:

Iowa Attorney General's Office, Director of Consumer Protection Division, 1305 E. Walnut Street, Des Moines, IA 50319, 1-515-281-5926, www.iowattorneygeneral.gov.

For Residents of Maryland

You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, http://www.marylandattorneygeneral.gov/.

For Residents of New Mexico

New Mexico consumers have the right to obtain a security freeze or submit a declaration of removal.

You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

(1) the unique personal identification number, password or similar device provided by the consumer reporting agency;

(2) proper identification to verify your identity; and

(3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of pre-screening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

For Residents of New York

You may also obtain information about security breach response and identity theft prevention and protection from the New York Attorney General's Office:

Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, www.ag.ny.gov.

For Residents of North Carolina

You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6000, www.ncdoj.gov.

For Residents of Oregon

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. Contact information for the Oregon Department of Justice is as follows:

Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301, 1-877-877-9392, www.doj.state.or.us.