BakerHostetler

Baker&Hostetler LLP

811 Main Street
Suite 1100
Houston, TX 77002-6111

T 713.751.1600
F 713.751.1717
www.bakerlaw.com

Kimberly C. Gordy
direct dial: 713.646.1360
kgordy@bakerlaw.com

October 2, 2023

VIA EMAIL (IDTHEFT@OAG.STATE.MD.US)

Anthony G. Brown
Attorney General
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: *Incident Notification*

Dear Sir or Madam:

We are writing on behalf of our client, Chico's FAS, Inc. ("Chico's"), to provide notice to your office concerning a security incident involving two Maryland residents.

Chico's uses a staffing agency to place third-party contractors who provide customer telephone support at the Chico's call center. On August 8, 2023, Chico's became aware that one of those contractors was inappropriately capturing and using customer payment card information provided to him by customers placing orders through the call center. This individual was only employed at the call center for a short time, from May 22, 2023 to August 10, 2023, and was promptly terminated following the investigation into this incident.

Chico's reviewed this individual's customer service activity, including all phone orders he processed, to identify the customer information at issue. Based on Chico's review of this activity, they determined that the individual had access to the personal information of two Maryland residents, including their names and payment card numbers. Importantly, Social Security numbers and driver's license numbers were **not** involved in this incident, and this individual could not access individuals' online accounts with Chico's.

On October 2, 2023, Chico's mailed notification letters via First Class mail to the Maryland residents involved in accordance with Md. Code Ann., Com. Law § 14-3504. A copy of the notification letter is attached. Chico's has provided contact information for any questions individuals may have regarding the incident.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Kimberly C. Gordy
Partner

Enclosure

<Return Name>
<Return Address>
<City> <State> <Zip>

<FirstName> <LastName>
<Address1>
<Address2>
<City><State><Zip>

<date>

Dear <first name> <last name>,

At Chico's FAS, Inc. ("Chico's"), we are committed to protecting the privacy and security of the information we maintain. Regrettably, we recently addressed a security incident involving some of that information. This letter explains the incident and our response.

What Happened: Chico's uses a staffing agency to place third-party contractors who provide customer telephone support at our call center. On August 8, 2023, we became aware that one of those contractors was inappropriately capturing and using customer payment card information provided to him by customers placing orders through the call center. This individual was only employed at our call center for a short time, from May 22, 2023 to August 10, 2023, and was promptly terminated following the investigation into this incident.

What Information Was Involved: We reviewed this individual's customer service activity, including all phone orders he processed, to identify the customer information at issue. Based on our review of this activity, we determined that the individual answered your call to the contact center and had access to the information you provided over the phone, including your payment card information. Importantly, your Social Security number and driver's license number were **<u>not</u>** involved in this incident, and this individual could not access your online account with Chico's.

What We Are Doing: We take this matter very seriously and have terminated our relationship with the third-party contractor. We are also enhancing the security protocols we have in place with our contractors to further safeguard the information in our care.

What You Can Do: We encourage you to remain vigilant by reviewing your payment card account statements for any unauthorized activity. If you see charges or activity that you did not authorize, please contact the relevant financial institution or payment card company immediately.

For More Information. If you have questions about this incident, please contact our dedicated assistance team at APServiceCare@chicos.com.

Sincerely,
Joseph Biffar
Vice President, Asset Protection

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-888-378-4329
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 1000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 160, Woodlyn, PA 19094, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Chico's FAS, Inc. is located at 11215 Metro Parkway, Fort Myers, FL 33966 and can be contacted at the following phone number 888-855-4986.

Additional information for residents of the following states:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.