Frankfurt Kurnit Klein + Selz PC

Tanya Forsheit
2029 Century Park East, Suite 1060, Los Angeles, CA 90067
T (310) 579 9615 F (347) 438 2092
tforsheit@fkks.com

November 28, 2018

VIA E-MAIL (consumer@ag.iowa.gov)

Tom Miller, Attorney General
Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street,
Des Moines, Iowa 50319-0106

Re: Incident Notification

Dear Attorney General Tom Miller:

I write on behalf of Dunkin Brands Inc. ("DBI"). On or after October 31, 2018, DBI learned from a security vendor that third parties that obtained usernames and passwords from security breaches of other companies were using this information to attempt to log into Dunkin' DD Perks accounts. Although DBI did not experience a data security breach of its own internal systems and its security vendor stopped most of the attempted logins, third parties may have been able to access DD Perks accounts if users had the same username and password as those used in compromised accounts from other companies' security breaches.

DBI immediately launched an internal investigation and has been working with its security vendor to remediate this event and to help prevent this kind of event from occurring in the future. DBI forced a password reset that required all of the potentially impacted DD Perks account holders to log out and log back in to their account using a new password. It also has taken steps to replace any DD Perks stored value cards with a new account number, but retaining the same value that was previously present on those cards. It also reported the incident to law enforcement.

Based on the investigation, DBI believes that there may have been access to the following notice-triggering information of Iowa residents: first and last name, email address (username), and 16-digit DD Perks account numbers and DD Perks QR Codes.

On November 28, 2018, DBI will begin notifying those individuals who may have been affected by this incident via U.S. mail where possible or other authorized delivery method. For users for whom DBI has an email address and not a mailing address, this notification is being provided via email.

DBI is sending out notice to the approximately 497 Iowa residents currently known to have been affected by the incident, in substantially the same form as the letter attached hereto.

Please do not hesitate to contact me at 310-579-9615 if you have any questions regarding this matter.

Sincerely,

Tanya L. Forsheit

Tanya L. Forsheit

Enclosures

Processing Center • P.O. BOX 141578 • Austin, TX 78714

00003
R83250H

JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

November 28, 2018

Subject: Important Message Regarding DD Perks Account Security

Dear John Sample,

Dunkin Brands Inc. ("Dunkin'") is writing to provide you with information regarding a recent incident involving your DD Perks account. Although Dunkin' did not experience a data security breach involving its internal systems, we've been informed that third-parties obtained usernames and passwords through other companies' security breaches and used this information to log into some Dunkin' DD Perks accounts. One of these may have been your account and we want you to know what happened, as well as the steps we are taking to protect your personal information.

What Happened?

On October 31, 2018, we learned from one of our security vendors that a third-party may have attempted to log in to your DD Perks account. We believe that these third-parties obtained usernames and passwords from security breaches of other companies. These individuals then used the usernames and passwords to try to break in to various online accounts across the Internet. Our security vendor was successful in stopping most of these attempts, but it is possible that these third-parties may have succeeded in logging in to your DD Perks account if you used your DD Perks username and password for accounts unrelated to Dunkin'.

What Information Was Involved?

The information involved depends on what you had in your DD Perks account. Information these third-parties may have been able to access includes:

- Your first and last names,
- Email address (username), and
- Your 16-digit DD Perks account number and your DD Perks QR code

What We Are Doing

We immediately launched an internal investigation and have been working with our security vendor to remediate this event and to help prevent this kind of event from occurring in the future. As you know already, we forced a password reset that required all of the potentially impacted DD Perks account holders to log out and log back in to their account using a new password. We also have taken steps to replace any DD Perks stored value cards with a new account number, but retaining the same value that was previously present on those cards. We also reported the incident to law enforcement and are cooperating with law enforcement to help identify and apprehend those third-parties responsible for this incident.

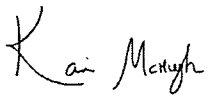
What You Can Do

As always, we strongly recommend that our guests create unique passwords for their DD Perks accounts, and do not reuse passwords used for their other unrelated online accounts. In addition, attached please find "Information about Identity Theft Protection." It includes steps you can take to help protect yourself against identity theft.

For More Information

If you have questions or concerns, please refer to dunkindonuts.com or call Consumer Care at 800-447-0013 during the following hours: Monday - Friday between 7AM and 7PM EST.

Sincerely,



Kari McHugh
Senior Director, Customer Relations
Dunkin' Brands, Inc.

Information about Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 9532	P.O. Box 6790
Atlanta, GA 30374-0241	Allen, TX 75013	Fullerton, CA 92834-6790
800-685-1111	888-397-3742	800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft. Residents of Maryland, North Carolina and Rhode Island may also obtain information about preventing and avoiding identity theft by contacting: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us; North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6400, www.ncdoj.gov; Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.

Fraud Alerts: There are two types of 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, which stays on your report for at least 90 days, if you suspect you have been, or are about to be, a victim of identity theft. You may have an extended alert placed on your credit report, which stays on for seven years, if you have already been a victim of identity theft with the appropriate documentary proof. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the toll-free numbers listed below:

Equifax	Experian	TransUnion
877-478-7625	888-397-3742	800-680-7289

Credit Freezes: You may have the right to put a credit freeze (or security freeze) on your credit file, 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. If you place a credit 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 credit freeze may delay your ability to obtain credit. Credit freeze laws vary from state to state, but there is no cost anywhere in the country for freezing or unfreezing your credit file. You must separately place a credit freeze on your credit file at each credit reporting company. Please contact the three major credit reporting companies as specified above for more information.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

02-02-3