SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK

THE PEOPLE OF THE STATE OF NEW YORK, by LETITIA JAMES, Attorney General of the State of New York, **Plaintiff,** **-against-** **DUNKIN' BRANDS, INC.,** **Defendant.**	Index No. 451787/2019 Hon. Barry R. Ostrager

CONSENT ORDER AND JUDGMENT

WHEREAS, the State of New York ("Plaintiff"), by its attorney, Letitia James, Attorney General of the State of New York ("NYAG"), filed a complaint on September 26, 2019 assigned to the Commercial Division of the Supreme Court of the State of New York, New York County, under the caption *People of the State of New York v. Dunkin' Brands, Inc.*, No. 451787/2019 (N.Y. Sup. Ct.), alleging that Dunkin' Brands, Inc. ("Dunkin'" or "Defendant") violated the New York General Business Law ("GBL") §§ 349, 350, and 899-aa, and the New York Executive Law § 63(12) in connection with its data security practices; and

WHEREAS, the parties have entered into the Consent and Stipulation (the "Stipulation"), dated September 15, 2020, which is hereby incorporated by reference into this Consent Order and Judgment (the "Consent Order"); and

WHEREAS, Defendant neither admits nor denies the NYAG's allegations in the complaint; and

WHEREAS, the parties consent to the entry of the following Consent Order for the purpose of resolving this action;

NOW, THEREFORE, IT IS ADJUDGED, ORDERED AND DECREED:

PARTIES SUBJECT TO JURISDICTION

1. This Consent Order shall extend to the NYAG, and to Defendant; anyone acting on Defendant's behalf, including its principals, officers, directors, employees, servants, successors or assignees; agents in active concert or participation with any of the foregoing who are involved in the conduct of business that is the subject of this litigation; and to any corporation, company, business entity, or other entity or device through which Defendant may now or hereafter act or conduct business that is the subject of this litigation.

DEFINITIONS

2. For the purposes of this Consent Order, the following definitions apply:

   a. "Customer" shall mean an individual with a Customer Account.

   b. "Customer Account" or "Account" shall mean a DD Perks or other account that has a username and password associated with it and is accessible through the Dunkin' website or mobile app.

   c. "Customer Personal Information" shall mean information that identifies or relates to an individual, including name, address, telephone number, email address, username and password, device ID, 16-digit DD Stored Value Card account number, PIN, or account balance of a DD Stored Value Card associated with a Customer Account.

d. "Customer Private Information" shall mean "private information," as defined in GBL § 899-aa(1)(b), of a Customer. For the avoidance of doubt, "Customer Private Information" shall include an unmasked DD Stored Value Card account number.

e. "Data Security Event" shall mean a credential stuffing attack, brute force attack, or hacking event involving unauthorized access to or acquisition of data that compromises the security, confidentiality, or integrity of Customer Personal Information.

f. "DD Stored Value Card" shall mean a Dunkin'-branded stored value card.

g. "Effective Date" shall mean the date this Consent Order is so-ordered by the Court.

h. "Eligible Customer" shall mean an Eligible 2015 Customer, Eligible 2018/19 Customer, Eligible 2020 Customer, Eligible NYAG Identified Customer, or Eligible Proactively Identified Customer.

i. "Historical Account Information" shall mean the following information:

i. All recorded instances of registration and de-registration of the Eligible Customer's DD Stored Value Cards, including the date and time of the event, that are known or available to Defendant;

ii. All transactions involving the Eligible Customer's DD Stored Value Cards, including the date and time of the transaction, location of the transaction, and amount used, that are known or available to Defendant; and

iii. All recorded instances in which the Eligible Customer's DD Stored Value Card account was reloaded, including the date and time of the event and the amount added, that are known or available to Defendant.

j. "New York Customer" shall mean a Customer who has either stated or indicated to Defendant that their state of residence is New York State.

k. "Notice Date" shall mean the last date on which letters or emails are sent to Eligible Customers pursuant to paragraphs 12, 13, and 14.

l. "Unauthorized Use" with respect to a DD Stored Value Card shall mean use or acquisition of a DD Stored Value Card without authorization.

3. For the purposes of this Consent Order, the following Customer class definitions shall apply:

a. "2015 Customer" shall mean a New York Customer from the list of approximately 19,715 Customers identified by SK C&C USA Inc. d/b/a CorFire in August 2015.

b. "2018/19 Customer" shall mean a New York Customer from the approximately 300,000 Customers impacted in the Data Security Events occurring from October 1, 2018 to January 31, 2019 and brought to Defendant's attention by Shape Security, Inc. in October and November 2018 and January 2019.

c. "2020 Customer" shall mean a New York Customer whose Account Defendant's personnel found had been, or reasonably believed may have been, accessed without authorization through a Data Security Event from January 1, 2020 to April 30, 2020.

d. "Eligible 2015 Customer" shall mean a 2015 Customer who has had a DD Stored Value Card associated with the Customer's Account between January 1, 2015 and the Effective Date, unless the 2015 Customer contacted Defendant during the 2015 calendar year concerning Unauthorized Use and whose complaint Defendant processed and resolved prior to the Effective Date.

e. "Eligible 2018/19 Customer" shall mean a 2018/19 Customer who had a DD Stored Value Card associated with the Customer's Account in October or November 2018, unless the 2018/19 Customer contacted Defendant in response to the notices of Unauthorized Use issued to the 2018/19 Customers in November 2018 and February 2019 and whose complaint Defendant processed and resolved prior to the Effective Date.

f. "Eligible 2020 Customer" shall mean a 2020 Customer who has had a DD Stored Value Card associated with the Customer's Account any time since January 1, 2020, unless the 2020 Customer contacted Defendant during the 2020 calendar year concerning Unauthorized Use and whose complaint Defendant processed and resolved prior to the Effective Date.

g. "Eligible Proactively Identified Customer" shall mean a Proactively Identified Customer, but shall not include a Proactively Identified Customer who contacted Defendant concerning Unauthorized Use and whose complaint Defendant processed and resolved prior to the Effective Date.

h. "Eligible NYAG Identified Customer" shall mean a New York Customer from the approximately 4,800 potential Customer Accounts identified by the NYAG and provided to Defendant in February 2020 who had a DD Stored Value Card associated with their Customer Account between January 1, 2015 and the Effective Date.

i. "Reset Password Customer" shall mean a 2015 Customer, 2018/19 Customer, and Proactively Identified Customer.

j. "Proactively Identified Customer" shall mean a New York Customer that Defendant's personnel found had, or reasonably believed may have had, their DD Stored Value

Card(s) taken or used without authorization from January 1, 2015 to the Effective Date and that did not contact Defendant regarding Unauthorized Use.

AFFIRMATIVE OBLIGATIONS

4. Defendant shall comply with NY Executive Law § 63(12), NY GBL §§ 349, and 899-aa.

5. Defendant shall not misrepresent its data security practices.

6. Defendant shall maintain a comprehensive information security program ("Security Program") designed to protect Customer Personal Information that includes, at a minimum, reasonable technological, administrative, and physical safeguards.

7. The Security Program must include reasonable measures to protect Customer Accounts against brute force and credential stuffing attacks.

8. In the event that Defendant has a reasonable suspicion that there has been a Data Security Event, Defendant shall promptly conduct a reasonable investigation aimed at determining whether the Data Security Event is ongoing, the cause and scope of the Data Security Event, the Customer Accounts that may have been affected, and the categories of Customer Personal Information that may have been accessed and/or acquired. Defendant must reasonably document the steps it takes to investigate any such potential Data Security Event and maintain this documentation for a period of at least five (5) years.

9. In the event that Defendant confirms or has the reasonable belief that Customer Personal Information was accessed or acquired without authorization through a Data Security Event ("Impacted Customers"), and the Customer Account (a) did not have a DD Stored Value Card, (b) had a masked DD Stored Value Card associated with it, or (c) had an unmasked DD

Stored Value Card associated with it but Customer Private Information was not accessed or acquired without authorization, Defendant shall reset the Customer Account passwords of the Impacted Customers, inform each Impacted Customer by email or letter that an unauthorized third party logged into (or if appropriate, may have logged into) the Customer's Account, and promptly respond to any requests by Impacted Customers, including any requests to refund unauthorized purchases.

10. In the event that Defendant confirms or has the reasonable belief that Customer Private Information was accessed or acquired without authorization through a Data Security Event ("Private Information Impacted Customers"), Defendant shall notify each Private Information Impacted Customer in the manner required by GBL § 899-aa, reset Private Information Impacted Customers' passwords, transfer the Private Information Impacted Customers' DD Stored Value Cards' account balance (if any) to new DD Stored Value Card account numbers (if any), and promptly respond to any requests by Private Information Impacted Customers to refund unauthorized purchases (if any).

11. Defendant shall, within thirty (30) days of the Effective Date, reset the password of each Reset Password Customer, unless prior to the Effective Date Defendant reset the Customer's password either in response to a Data Security Event or when processing and resolving an Unauthorized Use complaint.

12. Within thirty (30) days of the Effective Date, Defendant shall send Eligible Customers the letters and emails specified below:

a. the letter in Appendix A to each Eligible 2015 Customer;

b. the letter in Appendix B to each Eligible 2018/19 Customer;

c. the letter in Appendix C to each Eligible Proactively Identified Customer, unless Defendant contacted the Customer prior to the Effective Date and provided all of the information contained in the letter in Appendix C;

d. the email in Appendix D to each Eligible 2020 Customer, unless Defendant contacted the Customer prior to the Effective Date and provided all of the information contained in the letter in Appendix D; and

e. the email in Appendix E to each Eligible NYAG Identified Customer.

Defendant shall send the letters and emails referenced in this paragraph by mail if the Eligible Customer provided a postal address to Defendant, and also by email if the Eligible Customer provided an email address to Defendant.

13. Within thirty (30) days of the Effective Date, Defendant shall issue the emails specified below to each Reset Password Customer whose password was reset pursuant to paragraph 11, and to whom Defendant is not required to send a letter or email pursuant to paragraph 12:

a. the email in Appendix F to each 2015 Customer; and

b. the email in Appendix G to each 2018/19 Customer.

14. Within thirty (30) days of the Effective Date, Defendant shall issue the email in Appendix H to each 2020 Customer who is not an Eligible 2020 Customer, unless Defendant contacted the Customer prior to the Effective Date and provided all of the information contained in the email in Appendix H.

15. For a period of ninety (90) days following the Notice Date, Defendant shall enable Eligible Customers to make requests for Historical Account Information for DD Stored Value Cards registered to the Customer's Account at any time between January 1, 2015 and the Effective

Date (the "Relevant Period") by email and phone. Within three (3) business days of receiving the request, Defendant shall provide the Eligible Customer with Historical Account Information for the Relevant Period, to the extent that such information is not already available to the Eligible Customer at the time of the request through the transaction history in the Customer Account. Defendant shall provide the information specified above to the Eligible Customer by email, or by another reasonable means as requested by the Eligible Customer.

16. For a period of ninety (90) days following the Notice Date, Defendant shall enable Eligible Customers who have had a DD Stored Value Card to report the Unauthorized Use of their cards by email or phone. Defendant shall promptly provide complete refunds for all Unauthorized Use of DD Stored Value Cards reported pursuant to this paragraph, unless Defendant reasonably determines that the DD Stored Value Card was not acquired or used without authorization. Such determination may be based on the absence of any indicia of Unauthorized Use upon a reasonable review of the Eligible Customer's Account history. Such determination may not be solely based on an Eligible Customer's failure to provide information substantiating the Unauthorized Use.

17. Defendant shall, at least seven (7) days prior to sending letters and emails to Eligible Customers pursuant to paragraphs 12, 13, and 14, provide the NYAG with an electronic version of a spreadsheet containing, for each Reset Password Customer, 2020 Customer, and Eligible NYAG Identified Customer, the Customer's name, email addresses, and addresses, and the Data Security Events in which the Customer's Account was, or may have been, accessed.

18. Defendant shall, within one hundred and eighty (180) days of the Notice Date, provide the NYAG with an electronic version of a spreadsheet containing (i) each Eligible Customer who contacted Defendant to report the Unauthorized Use of their DD Stored Value Cards, (ii) whether

Defendant provided a refund to the Eligible Customer, (iii) the refund Defendant provided to the Eligible Customer, and (iv) if no refund was provided, the basis for Defendant's determination that the DD Stored Value Card was not acquired or used without authorization. Defendant may request that information submitted pursuant to this provision be exempt from Freedom of Information Law disclosure pursuant to Public Officer Law § 87(2)(d), and will reiterate this request in any cover letter to the NYAG.

MONETARY RELIEF

19. Defendant shall pay the State of New York $650,000 in penalties and costs within fourteen (14) days of the Effective Date of this Consent Order. Upon application by the NYAG showing that Defendant has failed to make the payment required by this Consent Order, the Court shall enter a judgment against Defendant for the amount outstanding plus interest at the statutory post-judgment rate of nine (9) percent per annum from the date of violation or nonpayment, and the NYAG shall have execution thereof. Payments shall be made pursuant to written payment processing instructions to be provided by the NYAG.

CONTINUING JURISDICTION

20. This Court shall retain jurisdiction of this action for the purpose of carrying out the terms of this Consent Order, to which jurisdiction Defendant consents solely for purposes of the enforcement of this Consent Order, and, except as provided in paragraph 21 below, any party to this Consent Order may apply to this Court for such other and further relief as may be necessary to effectuate the terms of this Consent Order, upon seven (7) days' notice.

NOTICE OF VIOLATIONS

21. If the NYAG believes that Defendant has failed to comply with a provision of paragraphs 4 through 18 of this Consent Order, and if in the NYAG's sole discretion the failure to comply does not threaten the health or safety of the citizens of New York or create an emergency requiring immediate action, then prior to taking legal action for any alleged failure to comply with the Consent Order the NYAG shall provide notice to Defendant. Defendant shall have fourteen (14) days from receipt of such notice (the "Notice Period") to provide a written response, including either a statement that Defendant believes it is in full compliance with the relevant provision or a statement explaining why it did not comply with the relevant provision, and how it has come into compliance or when it will come into compliance. Defendant shall not seek a declaratory judgment concerning any alleged failure to comply with the Consent Order during the Notice Period.

MISCELLANEOUS TERMS

22. Notwithstanding any provision to the contrary, if the Court determines that Defendant has violated this Consent Order, Defendant agrees that any statute of limitations and other time related defenses applicable to the alleged violations, and any claims arising from or relating thereto, are tolled from the date of this Consent Order.

23. Paragraphs 6 through 10 of this Consent Order shall be in effect for six (6) years from the Effective Date.

24. Any notices, statements, or other written documents required by this Consent Order shall be provided by overnight mail delivery service to the recipient at the addresses set forth below, unless a different address is specified in writing by the party changing such address:

For the NYAG, to:

Attn: Bureau Chief
Bureau of Internet and Technology
New York State Office of the Attorney General
28 Liberty Street
New York, New York 10005

For Dunkin' Brands, Inc., to:

Chief Legal Officer
Dunkin' Brands, Inc.
130 Royall Street
Canton, Massachusetts 02021

Any such notices, statements, or other written documents required by this Consent Order will also be provided by e-mail as a courtesy to a party that provides e-mail contact information following the Effective Date.

25. Defendant shall not state or imply, or cause to be stated or implied, that the NYAG has approved, sanctioned, or authorized any practice, act, or conduct of Defendant.

26. The failure of any party to exercise any right under any provision of this Consent Order shall not constitute a waiver of any rights of that party to enforce such provision prospectively.

27. Nothing in this Consent Order shall be construed as relieving Defendant of its obligation to comply with all applicable laws, regulations, and rules, or as granting permission to engage in any acts or practices prohibited by such law, regulation, or rule.

28. Nothing in this Consent Order shall be construed as precluding the NYAG from communicating with any Dunkin' Customer.

29. Nothing in this Consent Order or the corresponding Stipulation shall be construed to deprive any non-party of any private right or cause of action, including a consumer's ability to file a complaint with the NYAG. This Consent Order is not intended for use, and may not be used in,

any other proceeding or action and is not intended, and should not be construed, as an admission of any liability or wrongdoing by Defendant.

30. This Consent Order and the Stipulation between the parties sets forth all of the promises, covenants, agreements, conditions, and understandings between the parties, and supersedes all prior and contemporaneous agreements, understandings, inducements, or conditions, express or implied. There are no representations, arrangements, or understandings, oral or written, between the parties relating to the subject matter of this Consent Order that are not fully expressed herein or in the Stipulation.

31. If any clause, provision, or section of this Consent Order shall, for any reason, be held to be invalid, illegal, or unenforceable in any respect, such invalidity, illegality, or unenforceability shall not affect any other clause, provision, or section of this Consent Order, and this Consent Order shall be construed and enforced as if such invalid, illegal, or unenforceable clause, provision, or section had not been contained herein.

32. This Consent Order shall not be altered except by order of the Court.

33. This Consent Order shall be construed in accordance with the laws of New York.

34. The clerk is hereby directed to enter this Consent Order forthwith.

35. This Court's order and judgment dated _____ __, 2020 is hereby deemed a decision which shall be entered by the clerk of the court.

IT IS SO ORDERED.

Dated: _____ __, 2020

_____

The Honorable Barry R. Ostrager

New York Supreme Court Justice

APPENDIX A

Eligible 2015 Customers

Subject: Notice of Data Breach

Dear John Sample,

Dunkin' Brands, Inc. ("Dunkin'") is writing to you with some information regarding your DD Perks account, in connection with a recent legal settlement between the New York State Attorney General and Dunkin' ("Settlement"). We want you to know what happened with respect to a 2015 security incident described below, the steps we have already taken to protect your account, and further steps that you may take to protect your account, as well as to inform you of resources available to you if you believe there was unauthorized activity or charges in your account.

What Happened?

In 2015, Dunkin's then-mobile app vendor notified Dunkin' it believed unauthorized third parties may have logged into approximately 19,715 Dunkin' accounts, including yours, using usernames and passwords obtained elsewhere (not through any compromise of Dunkin's own internal systems). These malicious actors may have obtained your DD Perks account information, including stored value card numbers and PINs.

What Information Was Involved?

The information available, and potentially obtained, included first and last name, email address (username), 16-digit DD Perks account number, PIN, and in some cases, account balance(s).

What Have We Done?

We have since forced a password reset that required all of the impacted DD Perks account holders to log out and log back in to their account using a new, unique password. We also have taken steps to replace any DD Perks stored value card numbers currently saved to your account with a new account number.

What You Can Do

As always, we strongly recommend that you create unique passwords for your DD Perks accounts, and not reuse passwords for other unrelated online or mobile accounts. We also recommend that you review your DD Perks account transaction history for unauthorized charges, especially in and around August 2015. If you suspect that any unauthorized charges were made using your account, please contact a Dunkin' representative using the contact information below. In addition, attached please find "Information about Identity Theft Protection." It includes steps you can take to help protect yourself against identity theft.

Requesting Your Account History or Reporting Unauthorized Charges

Consistent with the terms of the Settlement, you may request a copy of your account history and/or report **any unauthorized activity you believe occurred in your account for the next 90 days**. To request a copy of your account history or report unauthorized charges made using your account, please contact a Dunkin' representative at 1-800-447-0013 or customerservice@dunkinbrands.com.

If you contact Dunkin' within the next 90 days, Dunkin' will provide a refund for any verified unauthorized charges that occurred due to this incident unless Dunkin' reasonably determines that the DD Perks stored value card was not acquired or used without authorization, or you previously received a refund.

For More Information

If you have questions or concerns, please refer to dunkindonuts.com or call Customer Care at 1-800-447-0013 during the following hours: Monday - Friday between 7AM and 7PM EST.

Sincerely,

[Dunkin' Representative]

APPENDIX B

Eligible 2018/2019 Customers

Subject: Supplemental Notice of Data Breach

Dear John Sample,

Dunkin' Brands, Inc. ("Dunkin'") is writing to you with some information regarding your DD Perks account, in connection with a recent legal settlement between the New York State Attorney General and Dunkin' ("Settlement"). We want to provide you with supplemental information about a security incident involving your DD Perks account that took place in either late 2018 or January 2019, of which we previously informed you; the steps we have already taken to protect your account; and further steps that you may take to protect your account, as well as to provide you with resources available to you if you believe there was unauthorized activity or charges in your account.

What Happened?

We previously notified you, in November 2018 or February 2019, that Dunkin's security vendor had identified usernames and passwords, including yours, that were likely obtained through other companies' security breaches (not through any compromise of Dunkin's own internal systems) and were made available on the Internet. Malicious actors used those usernames and passwords to obtain DD Perks account information, including stored value card numbers and PINs.

What Information Was Involved?

The information available, and potentially obtained, included first and last name, email address (username), 16-digit DD Perks account number, PIN, and in some cases, account balance(s).

Why Are We Sending You a Second Notice?

Dunkin' issued notices like this one at the time of the incident.

We are sending you this additional notification to clarify that your account was among those that Dunkin's security vendor determined with high likelihood were accessed by an unauthorized third party in October or November 2018 or in January 2019.

What Have We Done?

At the time of the incident, we instituted a forced password reset that required all of the impacted DD Perks account holders to log out and log back in to their account using a new, unique password. We also took steps to replace any account numbers associated with DD Perks stored value cards saved in your account at the time with a new account number.

What You Can Do

As always, we strongly recommend that you create unique passwords for your DD Perks accounts, and not reuse passwords for other unrelated online or mobile accounts. We also recommend that you review your DD Perks account transaction history for unauthorized charges, especially in and around October and November 2018 and January 2019. If you suspect that any unauthorized charges were made using your account, please contact a Dunkin' representative using the contact information below. In addition,

attached please find "Information about Identity Theft Protection." It includes steps you can take to help protect yourself against identity theft.

Requesting Your Account History or Reporting Unauthorized Charges

Consistent with the terms of the Settlement**,** you may request a copy of your account history and/or report **any unauthorized activity you believe occurred in your account for the next 90 days**. To request a copy of your account history or report unauthorized charges made using your account, please contact a Dunkin' representative at 1-800-447-0013 or customerservice@dunkinbrands.com.

If you contact Dunkin' within the next 90 days, Dunkin' will provide a refund for any verified unauthorized charges that occurred due to this incident unless Dunkin' reasonably determines that the DD Perks stored value card was not acquired or used without authorization, or you previously received a refund.

For More Information

If you have questions or concerns, please refer to dunkindonuts.com or call Customer Care at 1-800-447-0013 during the following hours: Monday - Friday between 7AM and 7PM EST.

Sincerely,

[Dunkin' Representative]

APPENDIX C

Eligible Proactively Identified Customers

Subject: Notice of Potential Unauthorized Activity in Your Account

Dear John Sample,

Dunkin' Brands, Inc. ("Dunkin'") is writing to you with some information regarding your DD Perks account, in connection with a recent legal settlement between the New York State Attorney General and Dunkin' ("Settlement"). We want you to know what may have happened with your account with respect to a possible security incident, the steps we have already taken to protect your account, and further steps that you may take to protect your account, as well as to provide you with resources available to you if you believe there was unauthorized activity or charges in your account.

What Happened?

Dunkin' identified potential unauthorized activity relating to your DD Perks account, which may have involved malicious actors logging in, using, and/or obtaining access to your DD Perks stored value card or other information in your account. The potential unauthorized activity involved circumstances unique to your account, which may have involved: unusual registration and de-registration activity associated with your DD Perks stored value card; potential unauthorized use of your DD Perks stored value card by another DD Perks account holder; and/or unusual transaction activity involving your DD Perks stored value card.

You may have discussed this potential unauthorized activity with Dunkin's Customer Care personnel in the past, but we are sending this notice in case you have not. If you have any questions as to why you are receiving this notice, please contact Customer Care as noted below for more information about your account and access to your transaction history.

What Information Was Involved?

The information available, and potentially obtained, included first and last name, email address (username), 16-digit DD Perks account number, PIN, and in some cases, account balance(s).

What Have We Done?

We have since forced a password reset that requires you to log out and log back in to your account using a new, unique password. Depending on the circumstances, we may also have frozen or refunded your DD Perks stored value card.

What You Can Do

As always, we strongly recommend that you create unique passwords for your DD Perks accounts, and not reuse passwords for other unrelated online or mobile accounts. We also recommend that you review your DD Perks account transaction history for unauthorized charges. If you suspect that any unauthorized charges were made using your account, please contact a Dunkin' representative using the contact information below. In addition, attached please find "Information about Identity Theft Protection." It includes steps you can take to help protect yourself against identity theft.

Requesting Your Account History or Reporting Unauthorized Charges

Consistent with the terms of the Settlement**,** you may request a copy of your account history and/or report **any unauthorized activity you believe occurred in your account for the next 90 days**. To request a copy of your account history or report unauthorized charges made using your account, please contact a Dunkin' representative at 1-800-447-0013 or customerservice@dunkinbrands.com.

If you contact Dunkin' within the next 90 days, Dunkin' will provide a refund for any verified unauthorized charges that occurred due to this incident unless Dunkin' reasonably determines that the DD Perks stored value card was not acquired or used without authorization, or you previously received a refund.

For More Information

If you have questions or concerns, please refer to dunkindonuts.com or call Customer Care at 1-800-447-0013 during the following hours: Monday - Friday between 7AM and 7PM EST.

Sincerely,

[Dunkin' Representative]

Appendix D

Eligible 2020 Customers

Subject: Notice of Data Breach

Dear John Sample,

Dunkin' Brands, Inc. ("Dunkin'") is writing to you with some information regarding your DD Perks account, in connection with a recent legal settlement between the New York State Attorney General and Dunkin' ("Settlement"). We want to provide you with information about potential unauthorized activity in your DD Perks account, the steps we have already taken to protect your account, and further steps that you may take to protect your account, as well as to provide you with resources available to you if you believe there was unauthorized activity or charges in your account.

What Happened?

Between January and April 2020, malicious actors logged into a number of Dunkin' accounts, including yours, using usernames and passwords obtained elsewhere (not through any compromise of Dunkin's own internal systems).

What Information Was Involved?

The information available, and potentially obtained, included your first and last name, email address (username), 16-digit DD Perks account number, PIN, and in some cases, account balance(s). Any stored value card number in your account was masked except for the last four digits.

What Have We Done?

At the time of the incident, you should have received an email from us that we had instituted a forced password reset that required all of the impacted DD Perks account holders to log out and log back in to their account using a new, unique password. Although Dunkin' masked all but the last four digits of your DD Perks stored value card when stored on our system, we also took steps to replace any account numbers associated with DD Perks stored value cards saved in your account at the time with a new account number.

What You Can Do

As always, we strongly recommend that you create unique passwords for your DD Perks accounts, and not reuse passwords for other unrelated online or mobile accounts. We also recommend that you review your DD Perks account transaction history for unauthorized charges. If you suspect that any unauthorized charges were made using your account, please contact a Dunkin' representative using the contact information below. In addition, attached please find "Information about Identity Theft Protection." It includes steps you can take to help protect yourself against identity theft.

Requesting Your Account History or Reporting Unauthorized Charges

Consistent with the terms of the Settlement**,** you may request a copy of your account history and/or report **any unauthorized activity you believe occurred in your account for the next 90 days**. To request a copy of your account history or report unauthorized charges made using your account, please contact a Dunkin' representative at 1-800-447-0013 or customerservice@dunkinbrands.com.

If you contact Dunkin' within the next 90 days, Dunkin' will provide a refund for any verified unauthorized charges that occurred due to this incident, unless Dunkin' reasonably determines that the DD Perks stored value card was not acquired or used without authorization, or you previously received a refund.

For More Information

If you have questions or concerns, please refer to dunkindonuts.com or call Customer Care at 1-800-447-0013 during the following hours: Monday - Friday between 7AM and 7PM EST.

Sincerely,

[Dunkin' Representative]

Appendix E

Eligible NYAG Identified Customers

Subject: Supplemental Notice of Data Breach

Dear John Sample,

Dunkin' Brands, Inc. ("Dunkin'") is writing to you with some information regarding the security of your DD Perks account, in connection with a recent legal settlement between the New York State Attorney General and Dunkin' ("Settlement"). We want to provide you with supplemental information about potential unauthorized activity in your DD Perks account which we previously informed you of in March 2020, the steps we have already taken to protect your account, and further steps that you may take to protect your account, as well as to provide you with resources available to you if you believe there was unauthorized activity or charges in your account.

What Happened?

We previously notified you, in March 2020, that usernames and passwords to a number of Dunkin' accounts, including yours, had been identified as being available on the Internet.

What Information Was Involved?

The information available, and potentially obtained, may have included first and last name, email address (username), 16-digit DD Perks account number, PIN, and in some cases, card numbers or account balance(s).

Why Are We Sending You a Second Notice?

Dunkin' issued notices like this one in March 2020. We are sending you this additional notification to make you aware of the Settlement, and notify you that you may be eligible for a refund.

What Have We Done?

As we previously mentioned in the first notice you received in March 2020, we instituted a forced password reset that required all of the impacted DD Perks account holders to log out and log back in to their account using a new, unique password.

What You Can Do

As always, we strongly recommend that you create unique passwords for your DD Perks accounts, and not reuse passwords for other unrelated online or mobile accounts. We also recommend that you review your DD Perks account transaction history for unauthorized charges. If you suspect that any unauthorized charges were made using your account, please contact a Dunkin' representative using the contact information below. In addition, attached please find "Information about Identity Theft Protection." It includes steps you can take to help protect yourself against identity theft.

Requesting Your Account History or Reporting Unauthorized Charges

Consistent with the terms of the Settlement**,** you may request a copy of your account history and/or report **any unauthorized activity you believe occurred in your account for the next 90 days**. To request a

copy of your account history or report unauthorized charges made using your account, please contact a Dunkin' representative at 1-800-447-0013 or customerservice@dunkinbrands.com.

If you contact Dunkin' within the next 90 days, Dunkin' will provide a refund for any verified unauthorized charges that occurred due to this incident, unless Dunkin' reasonably determines that the DD Perks stored value card was not acquired or used without authorization, or you previously received a refund.

For More Information

If you have questions or concerns, please refer to dunkindonuts.com or call Customer Care at 1-800-447-0013 during the following hours: Monday - Friday between 7AM and 7PM EST.

Sincerely,

[Dunkin' Representative]

Appendix F

2015 Customers

Subject: Your Dunkin' Account

YOUR PASSWORD HAS BEEN RESET

Dunkin' Brands, Inc. ("Dunkin'") is writing to you with some information regarding your DD Perks account, in connection with a recent legal settlement between the New York State Attorney General and Dunkin'("Settlement"). In 2015, Dunkin's then-mobile app vendor notified Dunkin' it believed unauthorized third parties may have logged into approximately 19,715 Dunkin' accounts, including yours, using usernames and passwords obtained elsewhere (not through any compromise of Dunkin's own internal systems) (the "Incident").

Although you did not have a DD Perks stored value card registered to your account at the time of the Incident, consistent with the terms of the Settlement and our policy, **we have forced a password reset and logged you out of your account**. You will need to update your password and log back in to your account with your new, unique password prior to accessing your DD Perks account online or via the mobile app. Please do not use a password or username and password combination that you use for other online or mobile accounts. **Please click here to update your password.**

Please note that password reset emails may take up to two hours to deliver based on your email provider.

If you have any questions, please contact Customer Care via dunkindonuts.com.

Appendix G

2018/2019 Customers

Subject: Your Dunkin' Account

YOUR PASSWORD HAS BEEN RESET

Dunkin' Brands, Inc. ("Dunkin'") is writing to you with some information regarding your DD Perks account, in connection with a recent legal settlement between the New York State Attorney General and Dunkin' ("Settlement"). In October and November 2018 and early 2019, Dunkin's security vendor identified that, between October and November 2018 and in January 2019, DD Perks accounts, including yours, were accessed using usernames and passwords likely obtained through other companies' security breaches (not through any compromise of Dunkin's own internal systems) (the "Incident"). Malicious actors used those usernames and passwords to potentially obtain your DD Perks account information. We provided notice in November 2018 and February 2019 to affected customers who had a stored value card registered to their DD Perks account at the time.

Although you did not have a DD Perks stored value card registered to your account at the time of the Incident, consistent with the terms of the Settlement and our policy, **we have forced a password reset and logged you out of your account**. You will need to update your password and log back in to your account with your new, unique password prior to accessing your DD Perks account online or via the mobile app. Please do not use a password or username and password combination that you already use for other online or mobile accounts. **Please click here to update your password.**

Please note that password reset emails may take up to two hours to deliver based on your email provider.

If you have any questions, please contact Customer Care via dunkindonuts.com.

Appendix H

2020 Customers

Subject: Your Dunkin' Account

YOUR PASSWORD HAS BEEN RESET

Dunkin' Brands, Inc. ("Dunkin'") is writing to you with some information regarding your DD Perks account, in connection with a recent legal settlement between the New York State Attorney General and Dunkin' ("Settlement"). Between January and April 2020, malicious actors logged into a number of Dunkin' accounts, including yours, using usernames and passwords obtained elsewhere (not through any compromise of Dunkin's own internal systems) (the "Incident").

Although you did not have a DD Perks stored value card registered to your account at the time of the Incident, consistent with the terms of the Settlement and our policy, at the time of the incident, **we forced a password reset and logged you out of your account**. If you have not already done so, you will need to update your password and log back in to your account with your new, unique password prior to accessing your DD Perks account online or via the mobile app. Please do not use a password or username and password combination that you already use for other online or mobile accounts. As always, we strongly recommend that you create unique passwords for your DD Perks accounts, and do not reuse passwords for other unrelated online or mobile accounts. **If you have not already updated your password, please click here to update your password.**

Please note that password reset emails may take up to two hours to deliver based on your email provider.

If you have any questions, please contact Customer Care via dunkindonuts.com.