

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

-----X
**THE PEOPLE OF THE STATE OF NEW YORK,
by LETITIA JAMES, Attorney General of the
State of New York,**

Plaintiff,

COMPLAINT

-against-

**Index No.
IAS Part**

DUNKIN' BRANDS, INC.,

Defendant.

-----X

Of Counsel:

KIM A. BERGER
Chief, Bureau of Internet and
Technology
CLARK P. RUSSELL
Deputy Chief, Bureau of Internet and
Technology
JORDAN S. ADLER
Senior Enforcement Counsel
JOHANNA N. SKRZYPCZYK
EZRA STERNSTEIN
Assistant Attorneys General
28 Liberty St.
New York, NY 10005
(212) 416-8433

NATURE OF THE ACTION

1. Plaintiff, the People of the State of New York, by Attorney General Letitia James (the “OAG”), brings this action pursuant to Executive Law § 63(12), General Business Law (“GBL”) Article 22-A, §§ 349 and 350, and GBL § 899-aa to remedy past and ongoing fraudulent, deceptive, and unlawful practices by Dunkin’ Brands, Inc. (“Defendant” or “Dunkin”).

2. Defendant owns and operates a well-known brand, Dunkin’ Donuts, and franchises Dunkin’ Donuts restaurants. There are over eight thousand Dunkin’ Donuts restaurants in the nation, including more than a thousand locations in New York.

3. For at least a decade, Defendant has sold Dunkin’-branded stored value cards that can be used to purchase beverages, food, and merchandise, both at Dunkin’ stores and online on the Dunkin’ website. Dunkin’ enables customers to register and manage these cards by creating a Dunkin’ user account online. To encourage customers to create accounts, Dunkin’ has represented that the company uses reasonable safeguards to protect customers’ personal information from loss, misuse, and unauthorized access and disclosure.

4. In 2015, Dunkin’s customer accounts were targeted in a series of online attacks. During this period, attackers made millions of automated attempts to access customer accounts. Tens of thousands of customer accounts were compromised. Tens of thousands of dollars on customers’ stored value cards were stolen.

5. Dunkin’ was aware of these attacks at least as early as May 2015. Indeed, over a period of several months during the summer of 2015, Dunkin’s app developer repeatedly alerted Dunkin’ to attackers’ ongoing attempts to log in to customer accounts. The vendor even provided Dunkin’ with a list of 19,715 customer accounts that had been accessed by attackers

over just a sample five-day period. Dunkin' itself identified dozens of other accounts that had been "taken over" by attackers.

6. Despite having promised customers that it would protect their personal information and company policies that required a thorough and deliberate investigation, Dunkin' failed to conduct an appropriate investigation into, and analysis of, the attacks to determine which customer accounts had been compromised, what customer information had been acquired, and whether customer funds had been stolen.

7. Worse still, Dunkin' failed to take *any* action to protect many of the customers whose accounts it knew had been compromised. Among other failures, Dunkin' did not notify its customers of the breach, reset their account passwords to prevent further unauthorized access, or freeze the stored value cards registered with their accounts.

8. Even after more than four years, Dunkin' has yet to conduct an appropriate investigation into the reported attacks or take appropriate action to protect its customers.

9. Moreover, following the attacks in 2015, Dunkin' failed to implement appropriate safeguards to limit *future* brute force attacks through the mobile app. The attacks, and customer reports of compromised accounts, continued.

10. In late 2018, a vendor notified Dunkin' that customer accounts had again been attacked, and that the attacks had resulted in the unauthorized access of more than 300,000 customer accounts. Although Dunkin' contacted impacted customers, Dunkin' did not disclose to these customers that their accounts had been accessed without authorization. Instead, Dunkin' falsely conveyed that a third party had "attempted," but failed, to log in to the customers' accounts. And Dunkin' falsely conveyed to some customers that the third party's attempts to log in may have failed because Dunkin's vendor had blocked them.

11. Dunkin's representation to consumers that it used reasonable safeguards to protect consumers' personal information, and the company's statements concerning the 2018 breach, were false and misleading and violated New York's consumer protection laws, Executive Law § 63(12) and GBL §§ 349 and 350. Dunkin' also violated New York's breach notification law, GBL § 899-aa, which requires that businesses disclose a breach of security to all New York State residents whose private information was, or is reasonably believed to have been, acquired without valid authorization.

12. The OAG seeks restitution for consumers as well as injunctive and equitable relief appropriate to redress Defendant's fraudulent, deceptive, and illegal conduct. In addition, the OAG seeks the imposition of civil penalties and reasonable costs of investigation and litigation.

PARTIES

13. Plaintiff is the People of the State of New York by their attorney, Letitia James.

14. Defendant Dunkin' Brands, Inc. is a Delaware corporation with its principal place of business at 130 Royall Street, Canton, Massachusetts 02021. The company operates the Dunkin' Donuts brand and franchises thousands of Dunkin' Donuts restaurants, which serve coffee and baked goods.

15. Defendant has transacted business in the State of New York and contracted to supply goods and services in New York. It has offered and sold Dunkin'-branded stored value cards to consumers in New York and has offered and provided consumers in New York with Dunkin' accounts and related services online, through a website and mobile app.

16. On November 5, 2018, the OAG sent Defendant a pre-litigation notice, pursuant to GBL Article 22-A, by certified mail, return receipt requested. Plaintiff also sent Defendant's counsel a copy of the pre-litigation notice by email on November 5, 2018.

JURISDICTION

17. This Court has jurisdiction pursuant to: (i) Executive Law § 63(12), under which the OAG is empowered to seek injunctive relief, restitution, damages, and other equitable relief, including disgorgement, when a person or business engages in repeated fraudulent or illegal acts or persistent fraud or illegality in the carrying on, conducting or transaction of business; (ii) GBL § 349(b), which authorizes the OAG to seek injunctive relief, restitution, civil penalties, and other equitable relief, including disgorgement, when a person or business engages in deceptive acts and practices in the conduct of any business, trade, or commerce; (iii) GBL § 350, which authorizes the OAG to seek injunctive relief, restitution, civil penalties, and other equitable relief, including disgorgement, when a person or business engages in false advertising in the conduct of any business, trade, or commerce; and (iv) GBL § 899-aa, which authorizes the OAG to seek injunctive relief, damages, civil penalties, and other equitable relief, including disgorgement, when a person or business fails to disclose a security breach to New York State residents whose private information was, or was reasonably believed to have been, acquired without authorization.

FACTUAL ALLEGATIONS

A. Customers Use Dunkin' Accounts to Register DD Cards

18. At least since 2007, Dunkin' has offered and sold Dunkin'-branded reloadable stored value cards. Dunkin' refers to these cards as "DD cards." Customers can use DD cards to purchase beverages, food, and merchandise, both at Dunkin' stores and online on the Dunkin' website. Many consumers, in New York and elsewhere, have purchased DD cards through the Dunkin' website, through the Dunkin' mobile app, and in Dunkin' stores.

19. Dunkin' enables customers to register and manage their DD cards through Dunkin' customer accounts. Customers create accounts by completing an online form, available

in the Dunkin' Donuts mobile app and on the Dunkin' website, www.dunkindonuts.com. The form requires that the customer enter, among other things, their email address, name, and a password. Consumers, in New York and elsewhere, have created and used Dunkin' accounts.

20. Customers with a Dunkin' account and one or more registered DD cards receive additional protections and are eligible for additional services. For example, if a DD card registered to an account is lost or stolen, Dunkin' can transfer the customer's balance to a new card.

21. Dunkin' also offers an "Auto Reload" feature that enables customers with an account to automatically reload a registered DD card using a credit card the customer has stored with the account. In addition, customers with a Dunkin' account can participate in Dunkin's loyalty program, DD Perks, which awards points for purchases made using a DD card.

22. Customers often use their Dunkin' accounts in conjunction with the Dunkin' app, a free mobile app for Android and iOS devices that Dunkin' offers for download through the Google Play Store and the Apple App Store. The app enables users with a Dunkin' account to purchase, register, manage, and reload DD cards; view account profile information and transaction history; and use a registered DD card to make in-store purchases without presenting the physical card.

23. The Dunkin' mobile app that was available to customers between 2012 and 2016 was developed by SK C&C USA Inc., d/b/a CorFire, a third-party app developer retained by Dunkin'. Between 2012 and 2016, CorFire maintained and enhanced the Dunkin' app. CorFire also operated computer servers that communicated with the Dunkin' app, which was necessary for the app's operation.

B. Dunkin' Failed to Take Appropriate Action After Learning That Customer Accounts Were Targeted in a Series of Brute Force Attacks

24. Beginning in early 2015, Dunkin's customer accounts were targeted in a series of "brute force attacks." "Brute force attacks" are repeated, automated attempts to gain access to accounts, often using usernames and passwords stolen through security breaches of other unrelated websites or online services.

25. Over the course of 2015, attackers made millions of attempts to log in to Dunkin' customer accounts by transmitting customer email address and password combinations to Dunkin' systems.

26. An attacker that gained access to a customer's account had the ability to:
- a. Use DD cards registered to the account to make purchases. If the customer had previously enabled Auto Reload, which automatically reloads registered DD cards when their balance gets low, the attacker could use the DD cards indefinitely;
 - b. Access the customer's DD card numbers and personal identification numbers ("PINs"). With that information, the attacker could sell the customer's DD cards online;
 - c. Leverage free beverage coupons and other promotions associated with the account; and
 - d. Access other account information that could be incorporated into future attacks, including phishing campaigns.

27. By May 2015, Dunkin' personnel had recognized that attackers were gaining access to customer accounts. An internal PowerPoint presentation from mid-May 2015 explained that the company had "experienced spikes in traffic" to the Dunkin' website that "appear[ed] to be automated brute force login attacks." The presentation noted that Dunkin' was

already aware of 750 customers whose accounts had been affected by “intruders . . . spending guests’ gift card balances on tangible goods.”

28. In June 2015, Dunkin’s app developer, CorFire, independently discovered that servers responsible for communicating with the Dunkin’ mobile app were receiving an unusually high volume of traffic. CorFire examined the incoming communications and found that the traffic had come from what appeared to be a single device repeatedly attempting to log in to customer accounts, using different login credentials with each attempt. These findings were consistent with a brute force attack.

29. In mid-June 2015, CorFire alerted Dunkin’ of the attack. CorFire reported that the attempts to log in using different customer credentials indicated that the attackers were potentially accessing Dunkin’ customers’ accounts.

30. Dunkin’ failed to take appropriate action after receiving CorFire’s report. Dunkin’ did not ask CorFire to attempt to identify which customer accounts had been accessed by the attackers. Indeed, Dunkin’ did not conduct any investigation into the scope of the attacks or whether accounts had been accessed without authorization.

31. To mitigate the attack, CorFire used a “blacklist” to track the mobile device identifier used by the attackers and block incoming traffic associated with that device. The blacklist was only a stopgap solution, however, as attackers could circumvent the blacklist by changing the device identifier they used.

32. In a June 23, 2015 email to Dunkin’, CorFire recommended “a deeper proactive discussion on security and DDOS¹ and how collectively we can guard against them” including a

¹ DDOS is an abbreviation of “distributed denial of service,” a type of attack intended to disrupt a computer server or service by flooding the target with Internet traffic.

“series of meetings” between CorFire, Dunkin’, and another Dunkin’ vendor responsible in part for operations of the Dunkin’ website. Dunkin’ never engaged in these discussions.

33. The attacks against Dunkin’ customer accounts continued over the next several weeks. CorFire continued to provide Dunkin’ with updates about the attacks.

34. On July 15, 2015, CorFire sent Dunkin’ a Powerpoint presentation entitled “Dunkin Mobile App Security – Recent Threats.” The document stated that there had been tens of thousands of attempts to access customer accounts since the first attack in June. It also explained that, as with the June attack, attackers had been rotating through a list of possible usernames, attempting to log in only once per account. The document reported that, since the attack in June, CorFire had identified and manually blacklisted additional devices associated with this traffic.

35. Dunkin’ again failed to take appropriate action after receiving CorFire’s report. The company did not conduct an investigation into the attack and did not ask CorFire to attempt to identify which customer accounts had been accessed by the attackers.

36. The CorFire presentation also contained a list of security enhancements that it recommended implementing to mitigate the attacks. The OAG’s investigation did not uncover any evidence that Dunkin’ pursued any of CorFire’s recommendations.

C. Dunkin’ Failed to Take Appropriate Action After Learning of Additional Attacks and 19,715 Accounts That Had Been Compromised

37. By mid-August 2015, CorFire had developed a reliable way to identify attackers’ traffic even if the attackers attempted to disguise themselves by rotating through different device identifiers.

38. CorFire found that each time the attackers attempted to access a customer account, the attackers transmitted a particular series of requests to the Dunkin’ systems. When

the login attempt was successful, these requests retrieved customer information, including the customer's name and email address, a unique identifier associated with the customer called the "profile id," and the card numbers and associated PINs for all DD cards registered to the customer's account.

39. CorFire subsequently conducted a search of its records to identify Dunkin' accounts that the attackers had accessed. The company found that over a sample five-day period, attackers had successfully logged in to 19,715 accounts.² At least 2,200 of these accounts belonged to New York residents.

40. Among the group of 19,715 customers CorFire identified, reports of fraud rose dramatically in August, precisely when CorFire determined the accounts had been compromised. Moreover, for the following two months, this group of 19,715 customers accounted for 30% of all customer reports of account takeover fraud that Dunkin' logged, even though the group represented well below 1% of all accountholders.

41. In late August 2015, CorFire presented Dunkin' with its analysis and findings. CorFire laid out the relevant facts for Dunkin, including the number of times attackers had attempted to access Dunkin' accounts since August 7, 2015 (approximately 5,400,000), the number of customers impacted over that five-day period (19,715), and CorFire's methodology for identifying attackers' traffic.

42. CorFire also reported that the attacks were ongoing. Attackers had made 750,000 attempts to access Dunkin' customer accounts in the ten-day period *after* CorFire had conducted its search for compromised accounts. Accounts that were compromised during this ten-day

² The 19,715 accounts CorFire identified included 52 duplicates, and therefore may constitute only 19,663 accounts.

period were not included in the list of 19,715 accounts that had been compromised earlier in the month.

43. CorFire also presented recommendations of specific security enhancements that would thwart brute force attacks.

44. Following the meeting, CorFire provided a Dunkin' employee with a list of the 19,715 accounts that had been compromised over the sample five-day period. CorFire also provided the Dunkin' employee with copies of the slides from the presentation.

45. Dunkin' failed to conduct even the most basic investigation after receiving CorFire's report. Dunkin' did not investigate whether the 19,715 accounts had been accessed without authorization, what customer information had been acquired, and whether customer funds had been stolen.

46. For example, Dunkin' failed to monitor whether any of the 19,715 customers CorFire identified had themselves reported fraudulent activity on their accounts. As described above, reports of fraud among these accounts rose dramatically immediately following the attack.

47. Dunkin' also failed to investigate whether attackers had compromised other Dunkin' accounts outside of the sample five-day period that CorFire examined. As a result, Dunkin' failed to identify other customer accounts that were accessed by attackers during the summer of 2015.

48. In addition, Dunkin' failed to take appropriate actions to protect the 19,715 customers whose accounts CorFire had identified, such as notifying the customers of the breach, resetting the account passwords to prevent further unauthorized access, or freezing DD cards registered with the accounts.

49. Customer reports of compromised accounts continued to rise following the August 2015 incident. Yet Dunkin' did not implement any of the security enhancements CorFire had recommended to thwart brute force attacks.

50. By early 2018, the number of customers per month reporting their account had been compromised was three to four times the volume of customer reports in August 2015. In January 2018 alone, more than 950 customers reported that their account had been compromised. During this time period, Dunkin' failed to implement appropriate safeguards to limit brute force attacks through the mobile app.

51. Finally, in late March 2018, Dunkin' engaged a security vendor to help block these types of automated attacks.

D. Dunkin' Has Failed to Take Appropriate Action After Identifying Other Compromised Accounts

52. In addition to the 19,715 accounts CorFire identified in August 2015, Dunkin's loss-prevention personnel have at times separately identified other customer accounts that have been "taken over" by attackers. In all of these cases, attackers who had gained access to the customers' accounts had used or stolen DD cards registered to those accounts.³

53. Dunkin' has not taken appropriate steps to protect some of these customers, such as notifying the customers of the breach, or resetting their account passwords to prevent further unauthorized access. Dunkin' has also failed to make many of these customers whole, either by replacing stolen DD cards or issuing refunds for stolen funds.

³ In the process, the attackers also retrieved customer information, including customer names, email addresses, profile ids, and DD card numbers and the associated PINs.

54. In addition, Dunkin' has failed to close attacker accounts that it identified. Some of these accounts have been used repeatedly to facilitate the unauthorized use and theft of DD cards.

55. For example, in early 2015 Dunkin' identified an account used by one attacker to register, in a single day, 25 DD cards stolen from other customers' accounts. Dunkin' did not close the attacker's account. The attacker then used that same account in May, November, and December 2015 to register an additional 15 DD cards that he had stolen from other customers.

E. Dunkin' Violated its Own Data Security Policies

56. Dunkin's conduct in response to CorFire's reports of attacks violated the company's own policies concerning data security incidents, found in the Dunkin' Computer & Data Security Incident Response Plan ("CDSIRP").

57. The CDSIRP defined an eight phase process for responding to a report of a potential "security incident." These phases included, for example, "triage," during which the company would assess the details, scope, and severity of the reported incident and make a formal "incident declaration" based on the results of that assessment; "analysis," during which the company would collect and analyze additional data; "containment" and "eradication," for containing and eradicating "signs and symptoms" of the incident; and "lessons learned," which included a formal meeting to discuss recommendations for the future. The CDSIRP also required company personnel to maintain detailed documentation concerning the company's response to the incident.

58. Under the CDSIRP, a "security incident" included, among other things, "elevated levels of anomalous traffic or suspicious activity" and "active intrusion attempts from external sources."

59. CorFire's reports of high-volume attacks targeting Dunkin's customer accounts fell within the scope of Dunkin's CDSIRP and should have triggered the CDSIRP's incident response process. However, following each report, Dunkin' failed to adhere to many aspects of the CDSIRP, including the investigation, analysis, notification, and documentation required by the plan.

F. Dunkin' Customer Service Representatives Misrepresented the Manner in Which Customers' Accounts Had Been Compromised

60. In 2015 and 2016, thousands of Dunkin' customers contacted Dunkin' to report fraudulent activity associated with their accounts, including the unauthorized use and theft of DD cards. Many of these customers had been impacted in brute force attacks.

61. Instead of disclosing that customer accounts had been targeted in brute force attacks, Dunkin' customer service personnel told many customers that the customers' own actions may have led to the fraudulent activity. In particular, customer service personnel advised many customers that the fraudulent activity could have been the result of a "phishing" attack.

62. In a typical phishing attack, an attacker sends an email that purports to be from a business or individual that the email recipient knows. The email recipient is tricked into providing her login credentials to the attacker.

63. These statements by customer service personnel were misleading because many customers' accounts had been compromised through brute force attacks, a fact Dunkin' had known since at least May 2015. Had Dunkin' disclosed that customer accounts had been compromised through a series of brute force attacks, customers concerned about Dunkin's data security practices would have stopped using their accounts.

G. Dunkin' Misled Customers Whose Accounts Were Compromised in Brute Force Attacks in 2018

64. In October and November 2018, Dunkin' customer accounts were again targeted in a series of brute force attacks. Attackers gained access to more than 300,000 Dunkin' customer accounts, including the accounts of more than 36,000 New York customers, and retrieved customer information, including customer names, email addresses, and the card numbers (and associated PINs) of DD cards registered to the accounts. DD cards were registered to more than 175,000 of these accounts.

65. A Dunkin' security vendor first notified Dunkin' of these attacks on October 5, 2018. The vendor described some of this traffic as "unmitigated," which indicated that the vendor had not blocked the traffic.

66. As with the attacks in 2015, Dunkin' did not investigate the attack and did not ask its security vendor to identify which customer accounts had been accessed by the attackers.

67. On October 31, 2018, the vendor, of its own accord, provided Dunkin' with an initial list of accounts that had been accessed by attackers. The vendor updated the list over the next several weeks as it identified additional accounts that had been impacted by the attacks.

68. In contrast to earlier incidents, here Dunkin' contacted impacted customers. However, Dunkin's communications were misleading. Instead of disclosing that customers' accounts had been accessed without authorization, Dunkin' falsely represented that it and its vendor had concluded only that a third party had "attempted" or "may have attempted to log in" to customers' accounts.

69. For example, in November 2018, Dunkin' sent an email to the more than 300,000 customers whose accounts had been accessed by attackers. The email included the following statement:

We are not aware of any issue with the Dunkin' Mobile App or websites however we *recently observed attempted login activity* on your Dunkin' Perks Account using a device not previously associated with your account. As a precaution, we have reset your Dunkin' Perks password . . .

(Emphasis added.)

70. A reasonable consumer would understand this to mean attackers had attempted to log in to the customer account but had not been successful. But that was not the case – Dunkin's vendor had determined that attackers had successfully logged in to the account of every customer that received this email.

71. Dunkin' also sent certain of these customers – the approximately 175,000 customers who had one or more DD cards registered to their account – a letter.⁴ The letter did not state that attackers had accessed the customer's account. Instead, the letter falsely represented that Dunkin's security vendor had merely found that a third party “may have attempted to log in” to the account:

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 . . . Our security vendor was successful in stopping most of these attempts, but *it is possible that these third-parties may have 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'.

(Emphasis added.)⁵

72. The letter also falsely represented that the attempt to log in to the customer's account may not have been successful, and that the attempt may not have been successful because Dunkin's security vendor had stopped it. In fact, precisely the opposite was true – for every customer that received Dunkin's letter, Dunkin's security vendor had determined not only

⁴ Dunkin' also reported the breach to the OAG as required by GBL § 899-aa.

⁵ The letter provided some of the categories of customer information that attackers “may have been able to access.” These included the customer's name, email address, and DD card number, which Dunkin' refers to as the customer's “account number.”

that it had failed to block the login attempt from reaching Dunkin's systems, but also that the login attempt had been successful.

73. This information – that an attacker has successfully logged in to the customer's account – is vitally important to consumers. Consumers who know that their account or account credentials have been compromised can take steps to protect themselves, for example by reviewing their accounts for fraudulent purchases or identifying accounts on other websites where the compromised credentials could be used to log in and changing the passwords to those accounts. Here, Dunkin's misleading statements made it less likely that customers would take such action.

74. Dunkin' issued replacement DD cards to those customers whose accounts had been impacted by the breach. However, Dunkin' did not refund customers for funds that had been stolen between the time the attacks began and the time the replacement cards were issued, a period of between one and two months, unless the customer proactively contacted Dunkin' and reported the fraud.

H. Dunkin' Has Misrepresented its Data Security Practices and Procedures

75. To encourage Dunkin' customers to create online accounts and use Dunkin's mobile app, Dunkin' has represented to consumers, expressly and by implication, that it provides reasonable safeguards to protect personal information from loss, misuse, and unauthorized access and disclosure.

76. For example, Dunkin's privacy policy, available on Dunkin's website and through Dunkin's mobile app, provided:

6. How We Protect Your Personal Information

Dunkin' Donuts has implemented **reasonable safeguards designed to prevent loss, misuse and unauthorized access, disclosure or modification of Personal Information provided or collected through**

our DD Online Services. With respect to payment card information and other Personal Information collected through our DD Online Services, we use Secure Socket Layer Technology or SSL to encrypt or scramble that information during transmission.

Unfortunately, no system or online transmission of data can be guaranteed to be 100% secure and you should always take appropriate security measures to protect your Personal Information, including ensuring that you have up-to-date antivirus software. If you believe that your Dunkin' Donuts account or any information you provided to us is no longer secure, please notify us immediately through the Contact Us information provided below.

(Emphasis added.) Dunkin' has required customers creating a customer account to agree to Dunkin's terms of use and privacy policy.

77. Moreover, statements on Dunkin's website acknowledge the importance consumers place on data security generally and on Dunkin's representations regarding its data security practices and procedures in particular. For example, a webpage on the Dunkin' website entitled "FAQs"⁶ included the following question and answer about signing up for DD Perks:

Is my personal information secure?

We go to great lengths to ensure the security of your personal information. Please refer to our **privacy policy**⁷ for all the details on how we use your data.

78. The FAQ webpage also included the following question and answer regarding purchasing DD cards:

Is it really safe to use my credit card to order from DunkinDonuts.com?

Yes. We use a sophisticated software program (Secure Socket Layer Technology or SSL) that encrypts all information before it's sent to us. If anyone does intercept data, they won't be able to read or use it. In addition, all payment info is stored within your account—never on your device.

⁶ "FAQs" is an abbreviation of "frequently asked questions."

⁷ The words "privacy policy" hyperlink to the webpage containing Dunkin's privacy policy.

Dunkin' Donuts is committed to keeping your personal information confidential. For more information, please see our **Privacy Policy**.⁸

79. Dunkin's representations were misleading and deceptive because, as described above, in numerous instances the company failed to use reasonable safeguards to protect personal information from loss, misuse, and unauthorized access and disclosure. These include, but are not limited to:

- a. Failure to take appropriate action to respond to reports of attacks on customer accounts, including repeatedly failing to conduct a reasonable investigation;
- b. Failure to take appropriate action after learning of customer accounts that had been accessed without authorization, including failing to protect impacted customers and failing to conduct a reasonable investigation; and
- c. Failure to implement appropriate technical safeguards to mitigate a known attack vector under active exploit.

**FIRST CAUSE OF ACTION PURSUANT TO
EXECUTIVE LAW § 63(12):
REPEATED AND PERSISTENT FRAUDULENT BUSINESS CONDUCT**

80. The OAG repeats and realleges paragraphs 1 through 79 as if fully set forth herein.

81. Executive Law § 63(12) authorizes the OAG to bring an action to enjoin repeated or persistent fraudulent business conduct.

82. As set forth above, Defendant has engaged in repeated and persistent fraudulent acts, including but not limited to:

⁸ The words "privacy policy" hyperlink to the webpage containing Dunkin's privacy policy.

- a. Misrepresenting to consumers, expressly and by implication, that it provided reasonable safeguards to protect consumers' personal information from loss, misuse, and unauthorized access and disclosure;
- b. Misrepresenting to consumers, expressly and by implication, the manner in which their accounts were compromised;
- c. Misrepresenting to consumers, expressly and by implication, that their accounts had not been accessed without authorization;
- d. Misrepresenting to consumers, expressly and by implication, its vendor's findings regarding third parties' attempts to access the consumers' accounts; and
- e. Misrepresenting to consumers, expressly and by implication, the success of third parties' attempts to access the consumers' accounts.

83. By these actions, Defendant has engaged in repeated and persistent fraudulent conduct in violation of Executive Law § 63(12).

**SECOND CAUSE OF ACTION PURSUANT TO EXECUTIVE LAW § 63(12):
VIOLATIONS OF GENERAL BUSINESS LAW § 349:
DECEPTIVE BUSINESS PRACTICES**

84. The OAG repeats and re-alleges paragraphs 1 through 79 and incorporates them by reference herein.

85. Executive Law § 63(12) authorizes the Attorney General to bring an action to enjoin repeated illegal acts or persistent illegality in the carrying on, conducting, or transaction of business.

86. GBL § 349 prohibits deceptive acts and practices in the conduct of any business, trade, or commerce or in the furnishing of any service in the state of New York.

87. Defendant has engaged in repeated and persistent deceptive acts and practices, including but not limited to:

- a. Misrepresenting to consumers, expressly and by implication, that it provided reasonable safeguards to protect consumers' personal information from loss, misuse, and unauthorized access and disclosure;
- b. Misrepresenting to consumers, expressly and by implication, the manner in which their accounts were compromised; and
- c. Misrepresenting to consumers, expressly and by implication, that their accounts had not been accessed without authorization;
- d. Misrepresenting to consumers, expressly and by implication, its vendor's findings regarding third parties' attempts to access the consumers' accounts; and
- e. Misrepresenting to consumers, expressly and by implication, the success of third parties' attempts to access the consumers' accounts.

88. By these actions in violation of GBL § 349, Defendant has engaged in repeated and persistent illegality in violation of Executive Law § 63(12).

**THIRD CAUSE OF ACTION PURSUANT TO EXECUTIVE LAW § 63(12):
VIOLATIONS OF GENERAL BUSINESS LAW § 350:
FALSE ADVERTISING**

89. The OAG repeats and re-alleges paragraphs 1 through 79 and incorporates them by reference herein.

90. Executive Law § 63(12) authorizes the Attorney General to bring an action to enjoin repeated illegal acts or persistent illegality in the carrying on, conducting, or transaction of business.

91. GBL § 350 prohibits false advertising in the conduct of any business, trade, or commerce or in the furnishing of any service in the state of New York

92. Defendant has engaged in repeated and persistent false advertising, including but not limited to:

- a. Misrepresenting to consumers, expressly and by implication, that it provided reasonable safeguards to protect consumers' personal information from loss, misuse, and unauthorized access and disclosure;
- b. Misrepresenting to consumers, expressly and by implication, the manner in which their accounts were compromised; and
- c. Misrepresenting to consumers, expressly and by implication, that their accounts had not been accessed without authorization;
- d. Misrepresenting to consumers, expressly and by implication, its vendor's findings regarding third parties' attempts to access the consumers' accounts; and
- e. Misrepresenting to consumers, expressly and by implication, the success of third parties' attempts to access the consumers' accounts.

93. By these actions in violation of GBL § 350, Defendant has engaged in repeated and persistent illegality in violation of Executive Law § 63(12).

**FOURTH CAUSE OF ACTION
VIOLATIONS OF GENERAL BUSINESS LAW § 349**

94. The OAG repeats and realleges paragraphs 1 through 79 as if fully set forth herein.

95. GBL § 349 prohibits deceptive acts and practices in the conduct of any business, trade, or commerce or in the furnishing of any service in the state of New York.

96. As set forth above, Defendant has engaged in deceptive acts and practices in violation of GBL § 349, including, but not limited to:

- a. Misrepresenting to consumers, expressly and by implication, that it provided reasonable safeguards to protect consumers' personal information from loss, misuse, and unauthorized access and disclosure;
- b. Misrepresenting to consumers, expressly and by implication, the manner in which their accounts were compromised; and
- c. Misrepresenting to consumers, expressly and by implication, that their accounts had not been accessed without authorization;
- d. Misrepresenting to consumers, expressly and by implication, its vendor's findings regarding third parties' attempts to access the consumers' accounts; and
- e. Misrepresenting to consumers, expressly and by implication, the success of third parties' attempts to access the consumers' accounts.

**FIFTH CAUSE OF ACTION
VIOLATIONS OF GENERAL BUSINESS LAW § 350**

97. The OAG repeats and realleges paragraphs 1 through 79 as if fully set forth herein.

98. GBL § 350 prohibits false advertising in the conduct of any business, trade, or commerce or in the furnishing of any service in the state of New York.

99. As set forth above, Defendant has engaged in false advertising in violation of GBL § 350, including, but not limited to:

- a. Misrepresenting to consumers, expressly and by implication, that it provided reasonable safeguards to protect consumers' personal information from loss, misuse, and unauthorized access and disclosure;

- b. Misrepresenting to consumers, expressly and by implication, the manner in which their accounts were compromised; and
- c. Misrepresenting to consumers, expressly and by implication, that their accounts had not been accessed without authorization;
- d. Misrepresenting to consumers, expressly and by implication, its vendor's findings regarding third parties' attempts to access the consumers' accounts; and
- e. Misrepresenting to consumers, expressly and by implication, the success of third parties' attempts to access the consumers' accounts.

**SIXTH CAUSE OF ACTION
VIOLATIONS OF GENERAL BUSINESS LAW § 899-aa**

100. The OAG repeats and realleges paragraphs 1 through 79 as if fully set forth herein.

101. GBL § 899-aa requires that businesses disclose, in the most expedient time possible and without unreasonable delay, a breach of security to all New York State residents whose private information was, or is reasonably believed to have been, acquired without valid authorization.

102. Furthermore, GBL § 899-aa requires that, in the event New York State residents are required to be notified of a breach, businesses also notify the OAG, the New York Department of State, and the New York Division of State Police.

103. As set forth above, Defendant has knowingly or recklessly violated GBL § 899-aa, including but not limited to:

- a. Failing to disclose a breach of security to New York State residents whose private information was, or is reasonably believed to have been, acquired without

authorization in or after 2015, and failing to notify the appropriate New York State agencies of the breach; and

- b. Failing to accurately disclose a breach of security to New York State residents whose private information was, or is reasonably believed to have been, acquired without authorization in 2018.

PRAYER FOR RELIEF


WHEREFORE, Plaintiff requests an order and judgment:

- a. Permanently enjoining Defendant from violating the laws of the State of New York, including Executive Law § 63(12) and General Business Law §§ 349, 350, and 899-aa;
- b. Directing Defendant to produce an accounting of monies lost by consumers in New York as a result of Defendant's fraudulent, deceptive, and illegal acts;
- c. Directing Defendant to make full restitution to consumers and pay damages caused, directly or indirectly, by the fraudulent, deceptive, and illegal acts complained of herein plus applicable pre-judgment interest;
- d. Directing Defendant to pay a civil penalty of \$5,000 for each violation of GBL Article 22-A, pursuant to GBL § 350-d;
- e. Directing Defendant to pay a civil penalty of \$10 for each knowing or reckless violation of GBL § 899-aa, pursuant to GBL § 899-aa(6);
- f. Directing Defendant to properly notify each New York residents whose private information was acquired without authorization;
- g. Directing such other equitable relief as may be necessary to redress Defendant's violations of New York law;

- h. Awarding Plaintiff costs of \$2,000 pursuant to CPLR § 8303(a)(6); and
- i. Granting such other and further relief as the Court deems just and proper.

New York, NY
September 26, 2019

Respectfully submitted,
Letitia James
Attorney General of New York

By 
KIM A. BERGER
Chief, Bureau of Internet and Technology
CLARK P. RUSSELL
Deputy Chief, Bureau of Internet and
Technology
JORDAN S. ADLER
Senior Enforcement Counsel
JOHANNA N. SKRZYPCZYK
EZRA STERNSTEIN
Assistant Attorneys General
28 Liberty St.
New York, NY 10005
(212) 416-8433