

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

MOGINRUBIN LLP
Daniel J. Mogin, Esq., Bar No. 95624
Jennifer M. Oliver, Esq., Bar No. 311196
Timothy Z. LaComb, Esq., Bar No. 314244
600 West Broadway, Suite 3300
San Diego, CA 92101
Tel: (619) 687-6611
Fax: (619) 687-6610
dmogin@moginrubin.com
joliver@moginrubin.com
tlacomb@moginrubin.com

(Additional counsel on signature page)

Counsel for Plaintiffs

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA

ROSS DICZHAZY and WESLEY
ETHERIDGE II, individually and on
behalf of all others similarly situated,

Plaintiffs,

v.

DICKEY’S BARBECUE
RESTAURANTS INC. dba
DICKEY’s BARBEQUE PIT, INC., a
Texas corporation; DICKEY’S
CAPITAL GROUP, INC., a Delaware
Corporation, and DOES 1-50.

Defendant.

Case No: '20CV2189 L MDD

CLASS ACTION COMPLAINT

1. Violation of the California Consumer Privacy Act [Cal. Civ. Code § 1798.150]
2. Violation of the California Unfair Competition Law [Cal. Bus. & Prof. Code § 17200, *et seq.*]
3. Negligence
4. Declaratory and Injunctive Relief

JURY TRIAL DEMANDED

1 Plaintiffs Ross Diczhazy and Wesley Etheridge II (“Plaintiffs”) bring this
2 action against Dickey’s Barbecue Restaurants, Inc., d/b/a Dickey’s Barbecue Pit,
3 and Dickey’s Capital Group, Inc. (collectively, “Dickey’s”), and Doe Defendants
4 1-50 (together with Dickey’s, “Defendants”) on behalf of themselves and all others
5 similarly situated, (i) alleging violations of the California Consumer Privacy Act
6 [Cal. Civ. Code § 1798.150], the California Unfair Competition Law [Cal. Bus. &
7 Prof. Code § 17200, et seq.]; and negligence, and (ii) seeking actual and statutory
8 damages and declaratory and injunctive relief, based on the data breach alleged
9 herein.

10 I. NATURE OF THE ACTION

11 1. Dickey’s is the fastest-growing BBQ chain in the United States and
12 has experienced substantial growth in recent years, with annual revenues of nearly
13 \$70 million. Because of lax security measures, it has also experienced a massive
14 data breach that resulted in theft of millions of credit card numbers and continued
15 for months on end.

16 2. From as early as May 2019 until at least September of 2020, around
17 three million credit card numbers were siphoned from over 150 Dickey’s locations
18 and listed for sale on the well-known dark web marketplace Joker’s Stash (the
19 “Data Breach”). This is not the first cyber attack Dickey’s has suffered in recent
20 years.

21 3. Contrary to the requirements of Cal. Civ. Code § 1798.82, Defendants
22 have not notified customers whose credit card numbers and personal identifying
23 information (PII) were stolen and sold because of the Data Breach. As a result,
24 affected consumers have not taken prophylactic action to protect their identity and
25 financial accounts, and will continue to suffer ongoing and imminent risk to their
26 personal information and assets.

27 4. Multiple reputable cyber-security researchers including Krebs,
28 Gemini Advisory, and Q6 Cyber have reported on the Data Breach, also known as

1 the “BlazingSun” breach, since the data set first appeared for sale in mid-October
2 2020. The Data Breach would have continued without Defendants’ detection had
3 these cyber security firms not issued public reports on the Joker’s Stash data for
4 sale.

5 5. According to those reports, the “BlazingSun” credit card numbers
6 offered for sale on the dark web belong to consumers in 35 states, with the highest
7 amount in California. Dickey’s has 66 locations in California, the second-largest
8 number outside of its native Texas.

9 6. Krebs has also reported that the Joker’s Stash hackers are advertising
10 a “valid rate” of between 90% and 100% for these cards, meaning almost all cards
11 are active and ripe for immediate financial fraud.

12 7. The investigations by these cyber-security firms and affected card-
13 issuing institutions have traced the origin of the Data Breach to Dickey’s. Cyber-
14 security firms have also identified the breached locations, which include Dickey’s
15 franchises in California where Plaintiffs have used their payment cards since
16 January 1, 2020. There are thousands of cards in “BlazingSun” from zip codes
17 surrounding that location and others in California, with more being released for
18 sale on an ongoing basis.

19 8. Almost all Dickey’s BBQ locations, including all Dickey’s locations
20 in California, are franchises. However, Dickey’s exercises decision-making
21 control over several key aspects of its franchisees’ businesses, including the
22 software used to take orders and accept card payments.

23 9. For example, according to publicly filed franchise disclosures,
24 Dickey’s has required its franchisees to purchase and use Spark Point-of-Sale
25 software and Smokestack sales data collection and reporting software since 2019.
26 Both products are owned by Spark Intelligence, Inc., a Texas corporation. Before
27 2019, Dickey’s required its franchisees to purchase and use Aloha Point-of-Sale
28 software, which is owned by NCR Corporation, a Maryland corporation.

1 10. This Data Breach clearly violates the California Consumer Privacy
2 Act (“CCPA”). According to CCPA Section 1798.150, “personal information”
3 includes an individual’s first name or first initial and his or her last name in
4 combination with account number or credit or debit card number, in combination
5 with any required security code, access code or password that would permit access
6 to an individual’s financial account, when either the name or the data elements are
7 not encrypted or redacted.

8 11. Individuals’ unredacted and unencrypted first and last names,
9 combined with their payment card numbers and security codes, were exfiltrated in
10 the Data Breach. The PII disclosed in the Data Breach is therefore protected by
11 the CCPA.

12 12. Defendants have failed to maintain reasonable security controls and
13 systems appropriate for the nature of PII they maintain, as required by the CCPA,
14 common law and other statutes. As explained below, Defendants knew or should
15 have known that (i) industry standard EMV chip technology, in which the customer
16 inserts a secure chip into the card reader rather than the merchant swiping a less
17 secure magnetic strip, was needed to adequately protect customers’ PII, and (ii)
18 that the magnetic strip technology being used was vulnerable to attack.

19 13. Defendants also failed to maintain proper measures to *detect* hacking
20 and intrusion. For example, Dickey’s did not learn that 3 million of its customers’
21 payment cards had been stolen until the hack was publicly reported by third parties
22 – at least 16 months after it began. Defendants should have had breach detection
23 protocols in place, which could have detected the breach and alerted customers
24 much sooner.

25 14. The viewing, theft, and attempted sale of California consumers’ PII
26 on the dark web has already occurred and cannot be cured.

27
28

1 15. Defendants knew or should have known that Plaintiffs’ and class
2 members’ PII was highly sought after by cyber criminals and that Plaintiffs and
3 class members would suffer significant harm if their PII was stolen.

4 16. Plaintiffs and class members entrusted Defendants with their valuable
5 PII and financial account information. Defendants owed Plaintiffs and class
6 members a duty to exercise reasonable care in protecting that valuable data from
7 unauthorized disclosure or access.

8 17. Defendants breached their duty of care and disregarded Plaintiffs’ and
9 class members’ privacy rights in the PII by failing to implement reasonable
10 security procedures and practices to protect Plaintiffs’ and class members’ PII,
11 which included neglecting to (i) implement security systems and practices
12 consistent with federal and state guidelines; (ii) implement security systems and
13 practices consistent with industry norms; (iii) timely detect the Data Breach; and
14 (iv) timely disclose the Data Breach to impacted customers.

15 18. Defendants also had a legal duty to take reasonable steps to protect
16 customers’ PII under applicable federal and state statutes, including Section 5 of
17 the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45, and the CCPA.

18 19. Because of the Data Breach, Plaintiffs and the classes (defined below)
19 have been injured and continued to be injured in several ways. Plaintiffs and class
20 members (i) face an imminent and ongoing risk of financial theft, identity theft and
21 similar cyber crimes; (ii) have expended or will expend time and money to protect
22 against further cyber crimes; (iii) have lost value in their PII; and (iv) did not
23 receive the benefit of their bargain with Defendants regarding data privacy.

24 20. Section 1798.150 of the CCPA permits class treatment because
25 Defendants (i) failed to maintain reasonable security measures and (ii) disclosed
26 Californians’ unencrypted and unredacted first names or first initials and last
27 names with unencrypted and unredacted credit card numbers and the security code
28 needed to access individuals’ financial accounts.

1 **III. PARTIES**

2 **A. Plaintiffs**

3 26. Plaintiff Ross Diczhazy is a California citizen who resides in this
4 District. Mr. Diczhazy used his personal payment card to make a purchase from a
5 Dickey’s Barbeque location subject to the Data Breach on at least one occasion
6 since January 1, 2020.

7 27. Plaintiff Wesley Etheridge II is a California citizen who resides in this
8 District. Mr. Etheridge used his personal payment card to make a purchase from a
9 Dickey’s Barbeque location subject to the Data Breach on at least one occasion
10 since January 1, 2020.

11 **B. Defendants**

12 28. Defendant Dickey’s Capital Group, Inc. is a Delaware corporation
13 with its principal place of business at 18583 N. Dallas Parkway, Suite 120, Dallas,
14 Texas 75287. Dickey’s Capital Group is the holding company of Dickey’s
15 Barbecue Restaurants, Inc., and has an estimated value of \$400 million.

16 29. Defendant Dickey’s Barbecue Restaurants, Inc., d/b/a Dickey’s
17 Barbeque Pit, is a Texas corporation with its principal place of business at 4514
18 Cole Avenue, Suite 1015, Dallas, Texas 75205. Dickey’s Barbecue Restaurants,
19 Inc. is the franchisor of restaurants known as Dickey’s Barbecue Pits. Dickey’s
20 Barbecue Restaurants, Inc. is a wholly owned subsidiary of Dickey’s Capital
21 Group, Inc.

22 30. Defendant Dickey’s Capital Group, Inc. and Defendant Dickey’s
23 Barbecue Restaurants, Inc., d/b/a Dickey’s Barbeque Pit are hereafter collectively
24 as “Dickeys” or the “Dickey’s Defendants”.

25 31. The Dickey’s Defendants’ conduct was authorized, ordered, or
26 performed by their directors, officers, managers, agents, employees, or
27 representatives in the course of their employment and while actively engaged in
28 the management of Defendants’ affairs.

1 officer presiding over this action and the members of their immediate family and
2 judicial staff, and any juror assigned to this action.

3 36. Class Identity: The members of the classes are readily identifiable and
4 ascertainable. Defendants and/or their affiliates, franchisees, vendors, payment
5 processors, point-of-sale-software dealers, and card-issuing institutions, among
6 others, have contact information for Dickey's customers which can be used to
7 identify class members.

8 37. Numerosity: The members of the classes are so numerous that joinder
9 of all of them is impracticable. While the exact number of class members is
10 unknown to Plaintiffs at this time, based on information and belief, the nationwide
11 class consists of approximately 3 million Dickey's customers whose data was
12 compromised in the Data Breach, and the California class consists of many
13 thousands of Dickey's customers whose data was compromised in the Data Breach.

14 38. Typicality: Plaintiffs' claims are typical of the claims of the members
15 of the classes because all class members were subject to the Data Breach and had
16 their PII exposed or accessed in the Data Breach.

17 39. Adequacy: Plaintiffs will fairly and adequately protect the interests of
18 the classes. Plaintiffs have no interests antagonistic to the interests of the classes
19 and are aligned with class members' interests because they were subject to the
20 same Data Breach as class members and face similar threats because of the Data
21 Breach. Plaintiffs have also retained competent counsel with significant
22 experience litigating complex class actions.

23 40. Commonality and Predominance: There are also questions of law and
24 fact common to the classes, which predominate over any questions affecting only
25 individual class members. These common questions of law and fact include,
26 without limitation:

- 27 a. Whether Defendants violated § 1798.150 of the CCPA;
28

- 1 b. Whether Defendants' violated Cal. Bus. & Prof. Code § 17200,
2 et seq.;
- 3 c. Whether Defendants owed Plaintiffs and class members a duty
4 to implement and maintain reasonable security procedures and
5 practices to protect their personal information;
- 6 d. Whether Defendants acted negligently in connection with the
7 monitoring and/or protection of Plaintiffs' and class members'
8 PII;
- 9 e. Whether Defendants breached their duty to implement
10 reasonable security systems to protect Plaintiffs' and the
11 classes members' PII;
- 12 f. Whether Defendants' breach of their duty to implement
13 reasonable security systems directly and/or proximately caused
14 damages to Plaintiffs and class members;
- 15 g. Whether Defendants adequately addressed and fixed
16 vulnerabilities that permitted the Data Breach to occur;
- 17 h. Whether and when Defendants learned of the Data Breach and
18 whether the response was adequate;
- 19 i. Whether Plaintiffs and other class members are entitled to
20 credit monitoring and other injunctive relief;
- 21 j. Whether Defendants provided timely notice of the Data Breach
22 to Plaintiffs and class members; and,
- 23 k. Whether class members are entitled to compensatory damages,
24 punitive damages, and/or statutory or civil penalties as a result
25 of the Data Breach.

26 41. Defendants have engaged in a common course of conduct and class
27 members have been similarly impacted by Defendants' failure to maintain
28 reasonable security procedures and practices to protect customers' PII, as well as
Defendants' failure to timely alert affected customers to the Data Breach.

42. Superiority: A class action is superior to other available methods for
the fair and efficient adjudication of the controversy. Class treatment of common

1 questions of law and fact is superior to multiple individual actions or piecemeal
2 litigation. Absent a class action, most if not all class members would find the cost
3 of litigating their individual claims prohibitively high and have no effective
4 remedy. The prosecution of separate actions by individual class members would
5 create a risk of inconsistent or varying adjudications with respect to individual
6 class members and risk inconsistent treatment of claims arising from the same set
7 of facts and occurrences. A class action presents far fewer management
8 difficulties, conserves judicial resources and the parties' resources, and protects
9 the rights of each class member.

10 **V. FACTS ALLEGED**

11 **A. Background**

12 43. The term "dark web" refers to the part of the internet that is not
13 indexed by search engines. It is a hotbed of criminal activity. Individuals with
14 hardware and credentials to access live dark web sites can buy credit card numbers,
15 drugs, guns, counterfeit money, stolen subscription credentials, hacked Netflix
16 accounts and software that helps you break into other people's computers, among
17 other things.

18 44. The dark web helps ensure users' privacy by effectively hiding server
19 or IP details from the public. Users need special software to access the dark web.
20 Most websites on the dark web are not directly accessible via traditional searches
21 on common search engines and are therefore accessible only by users who know
22 the addresses for those websites.

23 45. The term "EMV" originally stood for "Eurocard, Mastercard, Visa,"
24 the three companies that created the modern security standard for credit and debit
25 card processing. When credit cards were first introduced, merchants used
26 mechanical card imprinters that required carbon paper to make an imprint. Later,
27 the magnetic strip method of processing was introduced.

28

1 46. Payment card magnetic strips contain the valuable card information
2 segregated into “tracks.” “Track 1” information includes the cardholder’s name,
3 expiration date, card verification balance or card verification code (“CVV or
4 CVC”), and account number, among other technical data needed to process the
5 transaction. “Track 2” information includes account number (the number on the
6 front of the card) expiration date, and other technical data needed to route and
7 process the transaction.

8 47. When magnetic strip technology is used, hardware electronically
9 contacts the card issuer, using information from the magnetic stripe to verify the
10 card and authorize the transaction. This process made illegal cloning of cards
11 relatively easier and more common because magnetic strips can be “skimmed.”
12 Skimming is a common scam in which fraudsters attach a tiny device, or
13 “skimmer,” to a card reader that intercepts and copies sensitive card information
14 from the magnetic strip. Thieves can then retrieve the stolen data and can either
15 clone the card or sell the card number to other scammers.

16 48. These inherent vulnerabilities led the payment card industry to
17 transition to chip-enabled EMV cards, which offer tighter security measures to
18 combat potential fraud and identity theft. However magnetic strips were not
19 replaced completely, merchants who lack readers to effectively process chip card
20 transactions can still swipe the magnetic strips on EMV cards.

21 49. EMV chips cannot be cloned or skimmed, and transmit data in an
22 encrypted format. They therefore offer much greater security against fraud
23 compared to magnetic stripe card transactions, which are prone to skimming and
24 rely on merchants’ inspection of the holder’s signature on the card itself.

25 50. In a debit or credit card purchase transaction, card data must flow
26 through multiple systems and parties to be processed, any of which may be
27 compromised by hackers if they are not secure. Magnetic strip technology does
28 not encrypt payment card information. Encryption limits security weaknesses by

1 converting sensitive card information into a non-readable format. By scrambling
2 the payment card data the moment it is captured, hackers who steal encrypted data
3 are left with hard to read or unreadable text in the place of payment card numbers
4 accompanying the cardholder’s personal information stored in the retailer’s
5 computers.

6 51. Use of magnetic strip technology to transmit payment is now well-
7 known to be antiquated and risky, and the major credit card companies have
8 developed and strongly encouraged EMV chips that increase security and better
9 protect against data breaches and theft.

10 52. Krebs estimates that more than 95% of stolen credit card data
11 currently available for purchase on the dark web was stolen via magnetic strip data,
12 which can be easily reproduced in counterfeit cards used for in-person payments.

13 53. The importance of using modern EMV chip technology rather than
14 magnetic strip technology may not be common knowledge for consumers, but it is
15 well-known to businesses accepting card payments.

16 54. For example, according to Mastercard’s “EMV/Chip Frequently
17 Asked Questions for Merchants,”

18 EMV secures the payment and reduces the
19 opportunities for fraudsters to steal data that can be
20 later used to counterfeit cards as fraudsters are
21 currently able to do with magnetic stripe cards. By
22 accepting chip payments, you are providing a more
23 secure transaction environment for your customers.
24 ... Basically, Chips cards are harder to clone or steal
25 data from. Accepting chip payments makes you
26 more attractive to customers because there are
27 generally more payment options at the terminal
(e.g., mobile, contactless or standard dip) and the
consumer will feel more confident when making a
purchase.”¹

28 ¹ <https://www.mastercard.us/content/dam/mccom/en-us/documents/merchant-emv-chip-faqs.pdf>

1 55. Defendants have long known that the use of magnetic strip processing
2 for payment card transactions is an unsecure payment method that puts their
3 customers' information at unnecessary risk. Yet, they failed to make the
4 investment to protect consumers' PII and financial accounts by upgrading to more
5 secure technology.

6 **B. The Data Breach**

7 56. On October 15, 2020, KrebsOnSecurity, a reputable cyber-security
8 firm, reported that more than three million stolen card records were being offered
9 for sale on a dark web marketplace called "Joker's Stash." According to Krebs,
10 Joker's Stash is "[o]ne of the digital underground's most popular stores for
11 peddling stolen credit card information."

12 57. On the same date, electronic data security company Gemini Advisory
13 also conducted an analysis of the records and determined that all three million
14 records in the "BlazingSun" set appear to be tied to purchases at a Dickey's
15 Barbecue Pit. This was later corroborated by other companies that track the sale
16 of stolen payment card data.

17 58. According to these reports, from as early as May 2019 until
18 September 2020, hackers utilized malware to intercept magnetic strip credit and
19 debit payments made at more than 150 Dickey's locations, including many
20 thousands of cards owned by California residents. More than half of the Dickey's
21 locations in California were impacted by this breach, including the location
22 Plaintiffs visited while the Data Breach was ongoing.

23 59. The first round of "BlazingSun" payment card records were uploaded
24 to Joker's Stash on October 12, 2020, and Joker's Stash has said it will continue to
25 release tranches of new card numbers obtained in the Data Breach on an ongoing
26 basis.

27 60. Joker's Stash claims that all available "BlazingSun" Data Breach
28 records contain all unencrypted data found in "Track 1" and "Track 2" of the cards'

1 magnetic strips. This includes the account owner’s name, account number,
2 expiration date, pin number, and the three- or four-digit “CVV” or “CVC” code.

3 61. According to Gemini, all the compromised payments were processed
4 using “the outdated magstripe method, which is prone to malware attacks.”

5 **C. Defendants’ Failure to Implement Reasonable Security**

6 62. Dickey’s exercises tight control over which payment systems
7 franchisees may employ. Dickey’s knew or should have known that outdated
8 magnetic strip systems would put their customer’s PII at risk. Nonetheless it failed
9 to implement modern EMV technology and instead allowed magnetic strip
10 payment card data to be used in many of its restaurants all over the country.

11 63. The Dickey’s Defendants also ignored Federal Trade Commission
12 (“FTC”) security guidelines and recommendations, which were put in place to help
13 entities protect PII and reduce the likelihood of data breaches.

14 64. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . .
15 practices in or affecting commerce,” including, as interpreted by the FTC, failing
16 to use reasonable measures to protect PII by companies like Defendants. Several
17 publications by the FTC outline the importance of implementing reasonable
18 security systems to protect data. The FTC has made clear that protecting sensitive
19 customer data should factor into virtually all business decisions.

20 65. In 2016, the FTC provided updated security guidelines in a
21 publication titled “Protecting Personal Information: A Guide for Business.” Under
22 these guidelines, companies should protect consumer information they keep; limit
23 the sensitive consumer information they keep; encrypt sensitive information sent
24 to third parties or stored on computer networks; identify and understand network
25 vulnerabilities; regularly run up-to-date anti-malware programs; and pay particular
26 attention to the security of web applications – the software used to inform visitors
27 to a company’s website and to retrieve information from the visitors.

28

1 70. Among other violations, Defendants violated their obligations under
2 Section 5 of the FTC Act. For example, Defendants did not learn of the breach
3 until it was publicly reported more than year after it commenced. This
4 demonstrates that Defendants do not (i) use an adequate intrusion detection system
5 to immediately expose a data breach; (ii) sufficiently monitor incoming traffic for
6 suspicious activity that indicates a hacker is trying to penetrate their systems; (iii)
7 properly monitor for the transmission of large amounts of data from their systems;
8 or (iv) maintain an appropriate plan to respond effectively to a data breach in the
9 event one occurs.

10 71. Plaintiffs would not have used their payment cards to make purchases
11 from Dickey's had they known the stores lacked adequate systems and practices to
12 safeguard customers' personal and financial information from theft.

13 **D. The Data Breach Caused Actual and Ongoing Damage to**
14 **Plaintiffs and Class Members**

15 72. As a direct and proximate result of Defendants' conduct, Plaintiffs
16 and the classes have been damaged and continue to suffer imminent and continuing
17 risk of harm from fraud and identity theft due to the Data Breach.

18 73. Once data is stolen, it can be exploited for profit or, as here, sold on
19 the dark web to someone who intends to exploit the data for profit. Hackers would
20 not expend the time and effort to steal PII and/or risk prosecution by listing it for
21 sale on the dark web if the PII was not valuable.

22 74. Malicious actors use PII to gain access to class members' digital life,
23 including bank accounts, social media, and credit card details. During that process,
24 hackers can harvest other sensitive data from the victim's accounts, including
25 personal information of family, friends, and colleagues.

26 75. Class members' PII can also be used to open unauthorized accounts
27 including financial accounts and utility accounts, obtain medical treatment using
28

1 victims' health insurance, file fraudulent tax returns, obtain government benefits,
2 obtain government IDs, or create "synthetic identities."

3 76. The PII accessed in the Data Breach therefore has significant value to
4 the hackers that have already sold or attempted to sell that information and may do
5 so again. In fact, names, addresses, valid credit card numbers, and "CVV" codes
6 are among the most valuable pieces of information for hackers.

7 77. The PII accessed in the Data Breach is also very valuable to Plaintiffs
8 and class members. For example, consumers use their unique and valuable PII to
9 access the financial sector, including when obtaining a mortgage, credit card, or
10 business loan. As a result of the Data Breach, Plaintiffs and class members' PII
11 has been compromised and lost significant value.

12 78. Plaintiffs and class members will face continuing risk of injury due to
13 the Data Breach for years to come. Perpetrators often wait months or years to use
14 the personal information obtained in data breaches, as victims often become
15 complacent and less diligent in monitoring their accounts after a significant period
16 has passed. Perpetrators will also re-use stolen personal information, meaning
17 individuals can be the victim of several cyber crimes stemming from a single data
18 breach. And there is often significant lag time between when a person suffers harm
19 due to theft of their PII and when they discover the harm. Plaintiffs and class
20 members will therefore need to continuously monitor their accounts for years to
21 ensure their PII obtained in the Data Breach is not used to harm them.

22 79. Plaintiffs and class members have expended and will continue to
23 expend time and effort to mitigate the actual and potential damage as a result of
24 the Data Breach, including actual payment card fraud and incurring significant
25 time and effort associated with closely reviewing and monitoring bank accounts
26 and credit reports for unauthorized activity for years to come.

27
28

1 80. On October 13, 2020, Dickey’s issued the following public statement:

2
3 We received a report indicating that a payment card
4 security incident may have occurred. We are taking this
5 incident very seriously and immediately initiated our
6 response protocol and an investigation is underway. We
7 are currently focused on determining the locations
8 affected and time frames involved. We are utilizing the
9 experience of third parties who have helped other
10 restaurants address similar issues and also working with
11 the FBI and payment card networks. We understand that
payment card network rules generally provide that
individuals who timely report unauthorized charges to the
bank that issued their card are not responsible for those
charges.

12 81. Dickey’s suggestion that its customers will not be damaged by the
13 theft of their valuable personal and financial information is wrong. Even where
14 customers have changed card numbers or been refunded for payment card fraud,
15 the theft of their PII cannot be cured. The PII disclosed in the Data Breach is the
16 exact type of data that hackers use to target victims for years through phishing and
17 other customized scams.

18 82. Plaintiffs and class members have expended and will continue to
19 expend significant time and money to reduce the risk of and protect against identity
20 theft caused by the Data Breach. According to the 2018 IBM/Ponemon Institute
21 study, where a consumer becomes a victim of identity theft and suffers \$1 or more
22 in direct or indirect losses, the average cost to the consumer is \$1,343.

23 83. Even when reimbursed for money stolen due to a data breach,
24 consumers are not made whole because the reimbursement fails to compensate for
25 the significant time and money required to repair the impact of the fraud. On
26 average, victims of identity theft spend 7 hours fixing issues caused by the identity
27 theft. In some instances, victims spend more than 1,000 hours trying to fix these
28 issues.

1 84. Victims of identity theft also experience harm beyond economic
2 effects. According to a 2018 study by the Identity Theft Resource Center, 32% of
3 identity theft victims experienced negative effects at work and 8% experienced
4 negative effects at school.

5 85. The U.S. Government Accountability Office likewise determined that
6 “stolen data may be held for up to a year or more before being used to commit
7 identity theft,” and that “once stolen data have been sold or posted on the web,
8 fraudulent use of that information may continue for years.”

9 86. Plaintiffs and the classes have therefore suffered and will continue to
10 suffer damages as a direct result of the data breach, including without limitation:

- 11 a. Theft of their personal and financial information;
- 12 b. Loss of use of and access to their compromised accounts;
- 13 c. Time spent reconfiguring automatic billing instructions;
- 14 d. Costs associated with the detection and prevention of identity theft
15 and the unauthorized use of their financial accounts, which are
16 currently being actively marketed for sale on the dark web;
- 17 e. Money and time spent to address actual and potential
18 consequences of the Data Breach, including searching for and
19 reporting fraudulent charges, cancelling and reissuing cards,
20 purchasing credit monitoring and identity theft protection services,
21 and the emotional distress of dealing with the consequences of the
22 Data Breach;
- 23 f. The imminent damages resulting from fraud and identity theft due
24 to their valuable PII and financial account information being sold
25 to criminals on the black market;
- 26 g. Damages to and diminution in value of their PII and financial
27 account information entrusted to Defendants with the
28 understanding that Defendants had reasonable and appropriate
 security measures in place to protect that information and/or would
 timely notify customers of any breach of that information;

- 1 h. Continued risk to their PII and financial accounts so long as
2 Defendants continue to fail to undertake appropriate and adequate
3 measures to protect Plaintiffs’ and class members’ data in their
4 possession; and
- 5 i. Continued and substantial future risk of being targeted for
6 phishing, data intrusion, and other illegal schemes based on their
7 payment card information because malicious actors use that
8 information to target victims of identity theft more effectively.

8 87. Plaintiffs and class members also suffered damage because they did
9 not receive the benefit of the bargain they struck when they entrusted their PII and
10 financial information to Defendants by making a payment card purchase at a
11 Dickey’s location. Defendants owed a duty of care to Plaintiffs and class members
12 including the obligation to provide reasonable and adequate data security for credit
13 and debit card payments, which Dickey’s failed to provide.

14 88. According to Krebs, as a direct and proximate result of Defendants’
15 conduct, “a significant amount of fraud related to these cards” has already
16 occurred. This will continue given that Dickey’s customers’ PII remains on sale
17 on the dark web, and more card numbers will reportedly be added on an ongoing
18 basis.

19 **VI. CLAIMS FOR RELIEF**

20 **COUNT I**

21 *(Against all Defendants on behalf of the California class)*

22 **Violation of the CCPA, Cal. Civ. Code § 1798.150**

23 89. Plaintiffs repeat and reiterate each of the allegations contained in the
24 paragraphs above as if fully set forth herein.

25 90. Defendants violated § 1798.150 of the CCPA by failing to prevent
26 Plaintiffs’ and class members’ nonencrypted and nonredacted personal information
27 from unauthorized access and exfiltration, theft, or disclosure as a result of
28

1 Defendants' violations of their duty to implement and maintain reasonable security
2 procedures and practices appropriate to the nature of the information.

3 91. Defendants have more than \$25 million in annual revenues and/or
4 receive the personal information of more than 50,000 consumers in California each
5 year. They are therefore subject to the CCPA.

6 92. Defendants collect consumers' personal information as defined in
7 Cal. Civ. Code § 1798.140. Defendants have a duty to implement and maintain
8 reasonable security procedures and practices to protect this personal information.
9 As identified herein, Defendants failed to do so. As a direct and proximate result
10 of Defendants' acts, Plaintiffs' and class members' unencrypted personal and
11 financial information was subjected to unauthorized access and exfiltration, theft,
12 or disclosure.

13 93. Plaintiffs and class members seek injunctive or other equitable relief
14 to ensure Defendants adequately safeguard customers' PII going forward, by
15 implementing reasonable security procedures and practices. This relief is
16 particularly important because Defendants continue to hold customers' PII,
17 including Plaintiffs' and class members' PII. Plaintiffs and class members have an
18 interest in ensuring that their PII is reasonably protected, and Defendants have
19 demonstrated a pattern of failing to adequately safeguard this information.

20 94. On November 2, 2020, Plaintiffs sent a notice letter to Defendants'
21 registered service agents via overnight post. Assuming Defendants cannot cure the
22 issues raised within 30 days, and Plaintiffs believe such cure is not possible under
23 these facts and circumstances, then Plaintiffs intend to promptly amend this
24 Complaint to seek actual and statutory damages as permitted by the CCPA.

25
26
27
28

1 **COUNT II**

2 *(Against All Defendants On behalf of the California class)*

3 **Violation of California’s Unfair Competition Law,**
4 **Cal. Bus. & Prof. Code § 17200, et seq.**

5 95. Plaintiffs repeat and reallege every allegation set forth in the
6 preceding paragraphs.

7 96. Defendants engaged in unlawful and unfair business practices in
8 violation of Cal. Bus. & Prof. Code § 17200, et seq.

9 97. As alleged herein, at minimum, Defendants engaged in the following
10 unlawful and/or unfair conduct: (i) violation of the CCPA; (ii) violation of Section
11 5 of the FTC act and related regulations concerning data security and (iii)
12 negligence.

13 98. As also alleged herein, Plaintiffs and class members were directly and
14 proximately harmed in several ways because of Defendants’ unlawful and/or unfair
15 conduct. Defendants are liable to Plaintiffs and class members for those damages.

16 **COUNT III**

17 *(Against all Defendants on behalf of all classes)*

18 **Negligence**

19 99. Defendants owed Plaintiffs and class members a duty to exercise
20 reasonable care in protecting their PII from unauthorized disclosure or access.
21 Defendants breached their duty of care by failing to implement reasonable security
22 procedures and practices to protect Plaintiffs’ and class members’ PII. Among
23 other things, Defendants failed to: (i) implement security systems and practices
24 consistent with federal and state guidelines; (ii) implement security systems and
25 practices consistent with industry norms; (iii) timely detect the Data Breach; and
26 (iv) timely disclose the Data Breach to impacted customers.

1 100. Defendants knew or should have known that Plaintiffs’ and class
2 members’ PII was highly sought after by cyber criminals and that Plaintiffs and
3 class members would suffer significant harm if their PII was stolen by hackers.

4 101. Defendants also knew or should have known that timely disclosure of
5 the Data Breach was required and necessary to allow Plaintiffs and class members
6 to take appropriate actions to mitigate the resulting harm. These efforts include,
7 but are not limited to, freezing accounts, changing passwords, monitoring credit
8 scores/profiles for fraudulent charges, contacting financial institutions, and
9 cancelling or monitoring government-issued IDs such as passports and driver’s
10 licenses. The risk of significant harm to Plaintiffs and class members (including
11 identity theft) increased as the duration of the Data Breach extended over more
12 than a year, and affected consumers still have not been notified.

13 102. Defendants had a special relationship with Plaintiffs and the class
14 members who entrusted Defendants with several pieces of PII. Customers were
15 required to provide PII when using a payment card to purchase Defendants’ goods
16 and/or services. Plaintiffs and class members were led to believe Defendants
17 would take reasonable precautions to protect their PII and would timely inform
18 them if their PII was compromised, but Defendants did not do so.

19 103. The harm that Plaintiffs and class members suffered (and continue to
20 suffer) was the reasonably foreseeable product of Defendants’ breach of their duty
21 of care. Defendants failed to enact reasonable security procedures and practices,
22 and Plaintiffs and class members were the foreseeable victims of data theft that
23 exploited the inadequate security measures. The PII accessed in the Data Breach
24 is precisely the type of information that cyber criminals seek and use to commit
25 cyber crimes.

26 104. But-for Defendants’ breach of their duty of care, the Data Breach
27 would not have occurred and Plaintiffs’ and class members’ PII would not have
28 been stolen and offered for sale by an unauthorized and malicious party.

COUNT IV

(Against all Defendants On behalf of all classes)

Declaratory Judgement

105. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

106. As described herein, an actual controversy has arisen and now exists as to whether Defendants had reasonable security measures in place under the CCPA.

107. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendants and third parties with similar inadequate security measures.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the classes, request the following relief:

A. A determination that this action is a proper class action under Federal Rule of Procedure Rule 23, certifying Plaintiffs as class representatives, and appointing the undersigned counsel as class counsel;

B. An award of compensatory damages, punitive damages, statutory and civil penalties to Plaintiffs and the classes as warranted by the CCPA and other applicable law;

C. Injunctive or other equitable relief that directs Defendants to provide Plaintiffs and the classes with free credit monitoring and to implement reasonable security procedures and practices to protect customers' PII that conform to federal and state guidelines and industry norms;

D. Declaratory judgement in favor of Plaintiffs determining that Defendants do not maintain reasonable security measures under the CCPA;

1 E. An award of reasonable costs and expenses incurred in prosecuting
2 this action, including attorneys’ fees and expert fees pursuant to Cal. Code Civ. P.
3 § 1021.5; and

4 E. Such other relief as the Court may deem just and proper.

5 **VIII. JURY DEMAND**

6 Pursuant to Fed. R. Civ. P. 38(b), Plaintiffs demand a trial by jury of all
7 issues properly triable to a jury in this case.

8
9 Dated: November 9, 2020

10 By: /s/ Daniel J. Mogin

11 **MOGINRUBIN LLP**

12 Daniel J. Mogin, Bar No. 95624
13 Jennifer M. Oliver, Bar No. 311196
14 Timothy Z. LaComb, Bar No. 314244
15 600 West Broadway, Suite 3300
16 San Diego, CA 92101
17 Tel: (619) 687-6611
18 Fax: (619) 687-6610
19 dmogin@moginrubin.com
20 joliver@moginrubin.com
21 tlacomb@moginrubin.com

22 **SCHACK LAW GROUP**

23 Alexander M. Schack, Bar No. 99126
24 Natasha N. Serino, Bar No. 284711
25 Shannon F. Nocon, Bar No. 316523
26 16870 West Bernardo Drive, Suite 400
27 San Diego, CA 92127
28 Tel: (858) 485-6535
Fax: (858) 485-0608
alexschack@schacklawgroup.com
natashaserino@schacklawgroup.com
shannonnocon@schacklawgroup.com

Counsel for Plaintiffs