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

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

I. NATURE OF THE ACTION

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

21. Plaintiffs and class members are therefore (i) entitled to actual and statutory damages under the CCPA and other laws, (ii) have incurred actual and concrete damages as a result of the unauthorized sale of their PII on the dark web, and (iii) face ongoing risks of disclosure of their PII in subsequent data breaches because Defendants have not demonstrated that they has implemented reasonable security systems and procedures.

22. Plaintiffs and class members have a significant interest in the protection and safe storage of their PII. They are further entitled to declaratory, injunctive, and other equitable relief necessary to protect their PII. This includes, but is not limited to, an order compelling Defendants to adopt reasonable security procedures and practices to safeguard customers' PII and prevent future data breaches.

II. JURISDICTION AND VENUE

23. This Court has jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 class members, and one or more members of the classes are residents of a different state than Defendants. The Court also has supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367.

24. This Court has personal jurisdiction over Defendants because Dickey's has over 60 locations in the State of California and has continuous and systematic contacts with and conducts substantial business in the State of California and this District.

25. Venue is proper in this District pursuant to 28 U.S.C. §1391(b). A substantial part of the events giving rise to these claims took place in this District. Dickey's has several locations within this District and Plaintiffs and numerous class members reside in this District and were therefore harmed in this District.

III. PARTIES

A. Plaintiffs

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

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

B. Defendants

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

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

30. Defendant Dickey's Capital Group, Inc. and Defendant Dickey's Barbecue Restaurants, Inc., d/b/a Dickey's Barbeque Pit are hereafter collectively as "Dickeys" or the "Dickey's Defendants".

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

32. The Dickey's Defendants, through their subsidiaries, divisions, affiliates and agents, operated as a single unified entity with each acting as the alter ego, agent or joint-venturer of or for the other with respect to the acts, violations, and common course of conduct alleged herein and under the authority and apparent authority of parent entities, principals and controlling parties.

33. Doe Defendants 1 through 50 are unknown persons who are in some manner responsible the wrongful conduct alleged herein. Plaintiffs will seek leave to amend this Complaint to state their true names when they are discovered.

IV. CLASS ACTION ALLEGATIONS

34. Plaintiffs bring this action on behalf of themselves and as a class action under Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure on behalf of the members of the following classes:

a) All California residents who made a purchase from Dickey's using a payment card, or otherwise disclosed payment card information to Dickey's, since January 1, 2020, and whose personal information was compromised including as part of the Joker's Stash BlazingSun data set (the "California class"); and

b) All persons who made a purchase from Dickey's using a payment card, or otherwise disclosed payment card information to Dickey's, since January 1, 2018, and whose personal information was compromised including as part of the Joker's Stash BlazingSun data set (the "Nationwide class").

35. Specifically excluded from the classes are Defendants; their officers, directors, or employees; any entity in which Defendants have a controlling interest; and any affiliate, legal representative, heir, or assign of Defendants. Also excluded from the classes are any federal, state or local governmental entities, any judicial

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

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

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

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

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

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

a. Whether Defendants violated § 1798.150 of the CCPA;

b. Whether Defendants' violated Cal. Bus. & Prof. Code § 17200, et seq.;

c. Whether Defendants owed Plaintiffs and class members a duty to implement and maintain reasonable security procedures and practices to protect their personal information;

d. Whether Defendants acted negligently in connection with the monitoring and/or protection of Plaintiffs' and class members' PII;

e. Whether Defendants breached their duty to implement reasonable security systems to protect Plaintiffs' and the classes members' PII;

f. Whether Defendants' breach of their duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiffs and class members;

g. Whether Defendants adequately addressed and fixed vulnerabilities that permitted the Data Breach to occur;

h. Whether and when Defendants learned of the Data Breach and whether the response was adequate;

i. Whether Plaintiffs and other class members are entitled to credit monitoring and other injunctive relief;

j. Whether Defendants provided timely notice of the Data Breach to Plaintiffs and class members; and,

k. Whether class members are entitled to compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the Data Breach.

41. Defendants have engaged in a common course of conduct and class members have been similarly impacted by Defendants' failure to maintain 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

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

V. FACTS ALLEGED

A. Background

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

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

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

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

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

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

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

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

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

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

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

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

54. For example, according to Mastercard's "EMV/Chip Frequently Asked Questions for Merchants,"

> EMV secures the payment and reduces the opportunities for fraudsters to steal data that can be later used to counterfeit cards as fraudsters are currently able to do with magnetic stripe cards. By accepting chip payments, you are providing a more secure transaction environment for your customers. … Basically, Chips cards are harder to clone or steal data from. Accepting chip payments makes you more attractive to customers because there are 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]

[1] https://www.mastercard.us/content/dam/mccom/en-us/documents/merchant-emv-chip-faqs.pdf

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

B. The Data Breach

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

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

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

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

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

magnetic strips. This includes the account owner's name, account number, expiration date, pin number, and the three- or four-digit "CVV" or "CVC" code.

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

C. Defendants' Failure to Implement Reasonable Security

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

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

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

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

66. The FTC recommends that businesses do not maintain payment card information beyond the time needed to process a transaction; restrict employee access to sensitive customer information; require strong passwords be used by employees with access to sensitive customer information; apply security measures that have proven successful in the particular industry; and verify that third parties with access to sensitive information use reasonable security measures.

67. The FTC also recommends that companies use an intrusion detection system to immediately expose a data breach; monitor incoming traffic for suspicious activity that indicates a hacker is trying to penetrate the system; monitor for the transmission of large amounts of data from the system; and develop a plan to respond effectively to a data breach in the event one occurs.

68. The FTC has brought several actions to enforce Section 5 of the FTC Act. According to its website:

> When companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up these promises. The FTC has brought legal actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information, or caused substantial consumer injury. In many of these cases, the FTC has charged the defendants with violating Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce. In addition to the FTC Act, the agency also enforces other federal laws relating to consumers' privacy and security.

69. Defendants were aware or should have been aware of their obligations to protect customers' PII and privacy before and during the Data Breach yet failed to take reasonable steps to protect customers from unauthorized access.

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

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

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

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

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

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

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

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

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

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

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

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

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

> We received a report indicating that a payment card security incident may have occurred. We are taking this incident very seriously and immediately initiated our response protocol and an investigation is underway. We are currently focused on determining the locations affected and time frames involved. We are utilizing the experience of third parties who have helped other restaurants address similar issues and also working with 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.

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

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

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

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

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

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

a. Theft of their personal and financial information;

b. Loss of use of and access to their compromised accounts;

c. Time spent reconfiguring automatic billing instructions;

d. Costs associated with the detection and prevention of identity theft and the unauthorized use of their financial accounts, which are currently being actively marketed for sale on the dark web;

e. Money and time spent to address actual and potential consequences of the Data Breach, including searching for and reporting fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, and the emotional distress of dealing with the consequences of the Data Breach;

f. The imminent damages resulting from fraud and identity theft due to their valuable PII and financial account information being sold to criminals on the black market;

g. Damages to and diminution in value of their PII and financial account information entrusted to Defendants with the 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;

h. Continued risk to their PII and financial accounts so long as Defendants continue to fail to undertake appropriate and adequate measures to protect Plaintiffs' and class members' data in their possession; and

i. Continued and substantial future risk of being targeted for phishing, data intrusion, and other illegal schemes based on their payment card information because malicious actors use that information to target victims of identity theft more effectively.

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

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

VI. CLAIMS FOR RELIEF

COUNT I

(Against all Defendants on behalf of the California class)

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

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

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

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

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

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

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

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

COUNT II

(Against All Defendants On behalf of the California class)

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

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

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

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

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

COUNT III

(Against all Defendants on behalf of all classes)

Negligence

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

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

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

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

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

104. But-for Defendants' breach of their duty of care, the Data Breach would not have occurred and Plaintiffs' and class members' PII would not have 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;

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

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

VIII. JURY DEMAND

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

Dated: November 9, 2020

By: */s/ Daniel J. Mogin*

MOGINRUBIN LLP
Daniel J. Mogin, Bar No. 95624
Jennifer M. Oliver, Bar No. 311196
Timothy Z. LaComb, 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

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

Counsel for Plaintiffs