Gayle M. Blatt, SBN 122048
gmb@cglaw.com
Jeremy Robinson, SBN 188325
jrobinson@cglaw.com
P. Camille Guerra, SBN 326546
camille@cglaw.com
CASEY GERRY SCHENK
FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, CA 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232

Attorneys for Plaintiff
and the proposed classes

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

MICHAEL MARHEFKA, on behalf of himself and a class of others similarly situated,

Plaintiff,

v.

DICKEY'S BARBECUE RESTAURANTS, INC., a Texas corporation,

Defendant.

Case No.: **'21CV585 GPC AGS**

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Michael Marhefka, individually, and on behalf of all others similarly situated, upon personal knowledge of the facts pertaining to him and on information and belief as to all other matters, by and through undersigned counsel, hereby brings this Class Action Complaint against Defendant Dickey's Barbecue Restaurants, Inc. ("Dickey's" or "Defendant"), and alleges as follows:

NATURE OF THE CASE

1. Plaintiff asserts this class action against Defendant Dickey's Barbecue Restaurants, Inc. for its failure to exercise reasonable care in securing and safeguarding their customers' personal identifying information ("PII"), including names, payment card numbers, payment card expiration dates, and payment card security codes.

2. On October 15, 2020, a daily blog that covers computer security and cybercrime, *KrebsOnSecurity.com*, revealed that payment card data had been stolen from Defendant's customers at more than 100 of Defendant's restaurant locations around the country (the "Data Breach").[1]

3. The article revealed that on October 12, 2020, a "dark web" payment card bazaar, "Joker's Stash," debuted a batch of more than three million stolen payment card records and advertised "valid rates" of between 90 to 100 percent. Companies that track the sale of stolen payment card data found one common theme among all the accounts for sale: They were used at one or more of Defendant's restaurants over the preceding 13 to 15 months, from May 2019 through September 2020.[2]

4. Gemini Advisory, a cyber intelligence firm, reported that approximately 156 of Defendant's locations across 30 states likely had payment systems compromised by payment card-stealing malware, with the highest

[1] Krebs on Security, *Breach at Dickey's BBQ Smokes 3M Cards*, *available at* https://krebsonsecurity.com/2020/10/breach-at-dickeys-bbq-smokes-3m-cards/#:~:text=KrebsOnSecurity%20has%20learned%20the%20data,card%20breach%20at%20Dickey's%20BBQ

[2] *Id.*

exposure in California and Arizona. Gemini Advisory also concluded that the payment transactions at Defendant's restaurants were processed via an outdated magstripe method, which is prone to malware attacks.[3]

5. Defendant is no stranger to data breaches. In 2015, Defendant experienced a ransomware attack that demanded $6,000 to return the company's marketing files. Following that attack, Defendant published an article detailing the incident and committing to a robust cybersecurity posture. The article, complete with security best practices and an endorsement of investing in proactive measures, featured quotes from then-CEO Laura Rea Dickey.[4]

6. Despite its past experience with data security incidents and promises to implement state of the art data security practices, Defendant again failed to protect its customers' PII with adequate data security.

7. Defendant could have prevented this Data Breach. In the past few years, there have been several data breaches at other restaurant chains and retail establishments resulting from malware installed on point-of-sale ("POS") systems. Indeed, the susceptibility of POS systems to malware is well-known throughout the restaurant industry. In the last five years, practically every major data breach involving retail stores or fast-food restaurant chains has been the result of malware placed on POS systems. Accordingly, data security experts have warned companies, "[y]our POS system is being targeted by hackers. This is a fact of 21st-century business."[5] Unfortunately, Defendant's decision to ignore warnings like this led to the damage alleged here.

8. In addition to Defendant's failure to prevent the Data Breach,

[3] Gemma Advisory, *Joker's Stash Breaches Dickey's Barbecue Pit*, *available at* https://geminiadvisory.io/jokers-stash-breaches-dickeys/

[4] Dickey.com, *DCEO: Guardians of the Network*, *available at* https://www.dickeys.com/press/in-the-news/dceo-guardians-of-the-network

[5] Datacap Systems Inc., *Point of sale security: Retail data breaches at a glance*, *available at* https://www.datacapsystems.com/blog/point-of-sale-security-retail-data-breaches-at-a-glance#.

Defendant also failed to *detect* the breach even though it lasted for more than a year.

9. The Data Breach was the result of Defendant's inadequate approach to data security and protection of its customers' PII that it collected during the course of business.

10. Defendant disregarded the rights of Plaintiff and the Class by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to disclose to its customers the material fact that it did not have adequate computer systems and security practices to safeguard PII, failing to take available steps to prevent the Data Breach, and failing to monitor and timely detect the Data Breach.

11. As a result of the Data Breach, Plaintiff's and Class members' PII has been exposed to criminals for misuse. The damages to Plaintiff and the Class include the following which have or may be suffered as a direct result of the Data Breach:

a. unauthorized charges on debit and credit card accounts;
b. theft of personal and financial information;
c. costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts;
d. damages arising from the inability to use debit or credit card accounts because accounts were suspended or otherwise rendered unusable as a result of fraudulent charges stemming from the Data Breach,
e. damages arising from the inability to withdraw or otherwise access funds because accounts were suspended, restricted, or otherwise rendered unusable as a result of the Data Breach, including, but not limited to, missed bill and loan payments, late-payment charges, and lowered credit scores and other adverse impacts on credit;
f. costs associated with spending time to address and mitigate the actual

and future consequences of the Data Breach such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, including, but not limited to, lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

g. the imminent and impending injury resulting from the potential fraud and identity theft posed by PII being exposed for theft and sale on the dark web

h. costs of products and services purchased at Defendant's various restaurants during the period of the Data Breach because Plaintiff and the Class would not have dined at Defendant's various restaurants had Defendant disclosed that it lacked adequate systems and procedures to reasonably safeguard PII; and

i. the loss of Plaintiff's and Class members' privacy.

12. The injuries Plaintiff and the Class suffered were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for PII.

13. Plaintiff and the Class members retain a significant interest in ensuring that their PII, which remains in Defendant's possession, is protected from further breaches, and seek to remedy the harms suffered as a result of the Data Breach for themselves and on behalf of similarly situated consumers whose PII was stolen.

JURISDICTION

14. Subject matter jurisdiction in this civil action is authorized pursuant to 28 U.S.C. § 1332(a) because the matter in controversy exceeds the sum or value of $75,000, exclusive of interest and costs, and is between citizens of different

states. Subject matter jurisdiction in this civil action is also authorized pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class members, at least one class member is a citizen of a state different from that of Defendant, and the amount in controversy exceeds $5 million, exclusive of interest and costs.

15. The Court has personal jurisdiction over Defendant because its contacts with the State of California are systematic, continuous, and sufficient to subject it to personal jurisdiction in this Court. More specifically, Defendant has purposefully availed itself of the privilege of conducting business in this state by selling and maintaining over sixty restaurant franchises here.

16. Venue is proper in this district pursuant to 28 U.S.C. § 1391 because a substantial part of the events and/or omissions giving rise to Plaintiff's and the Class members' claims occurred within this District. Numerous class members reside in this District and were therefore harmed in this District.

PARTIES

17. Plaintiff Marhefka is a citizen of the State of California and resides in West Covina, California.

18. Defendant Dickey's Barbecue Restaurants, Inc. is a Texas corporation with its principal place of business located at 4514 Cole Avenue, Suite 1015, Dallas, Texas 75205. Defendant operates a chain of corporate and franchise restaurants known as Dickey's Barbecue Pit.

FACTUAL BACKGROUND

A. Point-of-Sale Systems

19. The hospitality industry – restaurants, hotels, retail stores, and museums – utilize point-of-sale ("POS") terminals or devices to process customer payments for goods or services. Essentially, a POS terminal is a computerized version of a cash register. POS terminals consist of a computer with specific software programs that can record and track customer orders, process credit and debit card transactions, connect to other systems in a network, and manage

inventory.

20. When a credit or debit card is swiped at a POS terminal, the payment card data (or "PCD") contained within a payment card is read and briefly stored in the POS terminal's memory while passing through a number of systems and networks before ultimately reaching the retailer's payment processor.

21. PCD is stored in a POS system's memory in plain text and includes "Track 1" and "Track 2" data from the payment card. Tracks 1 and 2 data includes the cardholder's first and last name, the card's account number and expiration date, and the card's three-digit security code, known as the "CVV." This information, which can be used to clone credit/debit cards and to make purchases online or over the telephone, is unencrypted on the payment card and thus is unencrypted in the POS terminal's memory during processing.

22. POS systems are particularly vulnerable to malware – which is malicious software specifically designed to steal customer payment information. Attacks on POS systems began in 2005. Attackers use network-sniffing malware to intercept credit and debit card data during transmission to payment processors.

23. A malware attack is easy to implement and poses less risk to the attacker in terms of detection and capture as it can be installed remotely.

24. All-in-one POS systems are typically based on operating systems such as Windows Embedded, Windows XP and later versions, in addition to Unix operating systems, such as Linux. Thus, POS systems are highly susceptible to an array of attacks that can result in large data breach incidents.

25. For example, POS systems are vulnerable to "RAM-scraping" malware, which permit attackers to exfiltrate data found in memory while the data is processing inside the terminal. Software vulnerabilities are another problem where there is no longer support or patches for POS systems that have older running operating systems such as Windows XP or Windows XP Embedded.

B. Plaintiff's Transactions

26. On or about February 3, 2020; February 25, 2020; March 18, 2020; March 30, 2020; July 13, 2020; and July 27, 2020, Plaintiff Marhefka visited Dickey's Barbecue Pit, one of Defendant's affected restaurants, located at 1090 Huntington Drive in Duarte, using his payment card.

27. On or about February 24, 2020 and October 13, 2020, Plaintiff Marhefka visited Dickey's Barbecue Pit, one of Defendant's affected restaurants, located at 2363 E. Colorado Boulevard in Pasadena, using his payment card.

28. Plaintiff continues to monitor his account in an effort to detect and prevent misuse.

29. Since learning of the Data Breach, Plaintiff Marhefka has had to review his account statements for fraudulent charges.

30. Plaintiff would not have used his payment card to make purchases at Defendant's restaurants during the period of the Data Breach had Defendant disclosed that they lacked adequate computer systems and data security practices to safeguard customers' PII from theft.

31. Plaintiff suffered actual injury from having his PII stolen as a result of the Data Breach.

32. Plaintiff suffered actual injury and damages in paying money to, and purchasing products from, Defendant's restaurants during the Data Breach, expenditures which he would not have made had Defendant disclosed that they lacked computer systems and data security practices adequate to safeguard customers' PII from theft.

33. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and is concerned about the loss of his privacy.

34. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

35. Plaintiff has a continuing interest in ensuring his PII, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

C. Dickey's Customer Data Collection Practices

36. Defendant Dickey's Barbecue Restaurants, Inc. is a for-profit corporation with more than 483 restaurant locations in 43 states.

37. As part of the dining process, Defendant's restaurants, like most restaurants, accept payment cards through POS terminals, which accept customer payment card data and process it for payment at the time for which a meal is paid. This data includes the cardholder name, the account number, expiration date, card verification value ("CVV"), and PIN data for debit cards. Defendant stores this PII in the POS system and transmit this information to a third party for processing and completion of the payment.

38. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the PII collected, maintained, and stored in the POS systems is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud.

39. Such malware can go undetected for a long period of time, especially if industry best practices are not routinely used.

40. Card payment data in particular is a valuable commodity, and there is a "cyber black market" in which criminals openly post stolen payment card numbers for sale.

41. Legitimate organizations and the criminal underground alike recognize the value of PII contained in a merchant's data systems; otherwise, the latter would not aggressively seek or pay for it.

42. Professionals tasked with trying to stop fraud and other misuse know that PII has real monetary value in part because criminals continue their

efforts to obtain this data.[6] In other words, if any additional breach of sensitive data did not have incremental value to criminals, one would expect to see a reduction in criminal efforts to obtain such additional data over time. However, just the opposite has occurred. For example, the Identity Theft Resource Center reported 1,579 data breaches in 2017, which represents a 44.7 percent increase over the record high figures reported for 2016.

43. The PII of consumers remains of high value to identity criminals, as evidenced by the price criminals will pay through black-market sources, or what is often called the dark web. Experian reports that a stolen credit or debit card number can sell for $5–110 on the dark web.[7]

44. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding PII, and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on its customers as a result of a breach.

45. Defendant was, or should have been, fully aware of the significant volume of daily credit and debit card transactions at its restaurants, amounting to tens of thousands of daily payment card transactions, and thus, the significant number of individuals who would be harmed by a breach of Defendant's systems.

46. Unfortunately, and as alleged below, despite all of this publicly available knowledge of the continued compromises of PII in the hands of other third parties, such as retailers and restaurant chains, Defendant's approach to maintaining the privacy and security of Plaintiff's and Class members' PII was,

[6] CIO Magazine, *Data Breaches Rise as Cybercriminals Continue to Outwit IT*, *available at* http://www.cio.com/article/2686167/data-breach/data-breaches-rise-as-cybercriminals-continue-to-outwit-it.html, October 2016.

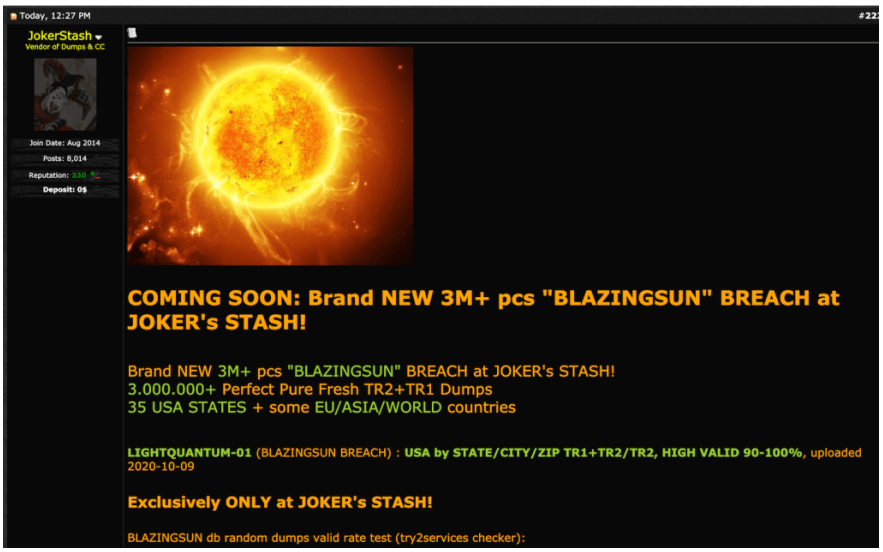
[7] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, *available at* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

reckless, or at the very least, negligent.

D. The Data Breach

47. On October 15, 2020, highly respected security blogger Brian Krebs reported that one of the dark web's most popular stores for selling stolen credit card information, "Joker's Stash," had begun selling a batch of more than 3 million new card records that had been used by customers at Defendant's restaurants around the country.[8]

48. "Joker's Stash" originally claimed that data from the breach would be available in August and again in September. On October 12, it debuted "BlazingSun," a compilation of three million stolen card records. "Joker's Stash" advertised the card payment information as having "valid rates" of between 90 to 100 percent.[9]



49. As explained by Krebs, the valid rates indicated that the breached merchant – Dickey's – was either unaware of the data compromise or had only just begun responding to it.[10]

50. Companies that track the sale in stolen payment card data, such as Q6 Cyber and Gemini Advisory, confirmed that the card-issuing financial institutions

[8] Krebs, *supra* note 1.
[9] *Id.*
[10] *Id.*

accounting with the accounts for sale in the BlazingSun batch had one common theme: All accounts were used at various Dickey's restaurants over the preceding 13 to 15 months.[11]

51. In its investigation of the Data Breach, Gemini Advisory concluded that the widespread nature of the breach indicated that the theft may be linked to a breach of Defendant's single central processor, which was used by a quarter of all of Defendant's restaurant locations.[12]

52. Gemini Advisory further reported that it had determined that the payment transactions at Defendant's restaurants were processed via the outdated magstripe method, which is prone to malware attacks.[13]

53. Gemini Advisory reported that the financial institutions they have been working with in connection with the Data Breach had already seen a significant amount of fraud related to those accounts.[14]

54. Following the previously alleged 2015 ransomware incident, Defendant published an article detailing the incident and committing to robust cybersecurity. That article set forth data security best practices and an endorsement of investing in proactive data security measures, featuring quotes from its CEO at the time.[15]

55. Despite Defendant's purported commitment to data security, the BlazingSun breach may contain as many as 3 million compromised card accounts with a median price of $17 per card.[16] This Data Breach dwarfs the 2015 ransomware incident.

56. In addition to Defendant's failure to prevent the Data Breach,

[11] Gemini Advisory, *supra* note 3.
[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] Dickey's.com, *supra* note 4.
[16] Gemini Advisory, *supra* note 3.

Defendant also failed to detect the breach for nearly 17 months. Intruders, therefore, had months to collect PII unabated. During this time, Defendant failed to recognize that its systems had been breached and that intruders were stealing data on millions of payment cards. Timely action by Defendant likely would have significantly reduced the consequences of the breach. Instead, Defendant took more than 17 months to realize that its systems had been breached, and thus contributed to the scale of the Data Breach and the resulting damages to Plaintiff and Class members.

57. While many merchants and vendors have responded to recent data breaches by adopting technology and security practices that help make transactions and stored data more secure, Defendant failed to do so. Instead, Defendant's restaurants continued to use the outdated magstripe method to process customers' purchases. This outdated magstripe method is prone to malware attacks.[17]

58. Additionally, based on information and belief, Defendant did not provide written notice to consumers affected by the POS malware attack.

E. Defendant Failed to Comply with Industry Standards

59. Despite the enumerated vulnerabilities of POS systems, available security measures, and reasonable business practices would have significantly reduced or even eliminated the likelihood that hackers could successfully infiltrate a business' POS system. The payment card networks (MasterCard, Visa, Discover, and American Express), data security organizations, state governments, and federal agencies have all implemented various standards and guidance on security measures designed to prevent these types of intrusions into POS systems. However, despite Defendant's understanding of the risk of data theft via malware installed on POS systems, and the widely available resources to prevent intrusion into POS data systems, Defendant failed to adhere to these guidelines and failed to

[17] *Id*.

take reasonable and sufficient protective measures to prevent the Data Breach.

60. Security experts have recommended specific steps that retailers should take to protect their POS systems. For example, a few years ago, Symantec recommended "point to point encryption" implemented through secure card readers, which encrypt credit card information in the POS system, preventing malware that extracts card information through the POS memory while it processes the transaction.[18] Moreover, Symantec emphasized the importance of adopting EMV (Europay, Visa, and Mastercard) chip technology. Datacap Systems, a developer of POS systems, recommended similar preventative measures.[19]

61. Credit card companies announced that retailers must use EMV chip reading machines by October 1, 2015 instead of swiping machines. EMV payment cards contain a microchip that is used to improve payment security and prevent counterfeit card fraud. Consumers insert their cards into the front of a card reader with the metallic square chip facing up instead of swiping cards. Cards with magnetic strips contain unchanging data that can easily be replicated over and over again, unlike the chip cards that create a unique transaction code that cannot be used again. If an attacker steals the chip data from a specific point of sale, card duplication is unavailable because the stolen transaction number created would not be usable again.

62. Upon information and belief, Defendant failed to use EMV chips at many of its restaurants to process customers' transactions, and instead used an outdated magstripe method. The outdated magstripe method used by Defendant is prone to malware attacks.[20]

---

[18] Symantec, *A Special Report On Attacks On Point-of-Sale Systems*, p. 3 (Nov. 20, 2014), *available at* https://docs.broadcom.com/doc/attacks-on-point-of-sale-systems-en

[19] DataCap Systems, *supra* note 5.

[20] Gemini Advisory, *supra* note 3

63. The major payment card industry brands set forth specific security measures in their Card (or sometimes, Merchant) Operating Regulations. Card Operating Regulations are binding on merchants and require merchants to: (1) protect cardholder data and prevent its unauthorized disclosure; (2) store data, even in encrypted form, no longer than necessary to process the transaction; and (3) comply with all industry standards.

64. The Payment Card Industry Data Security Standard ("PCI DSS") is a set of requirements designed to ensure that companies maintain consumer credit and debit card information in a secure environment.[21]

65. The PCI DSS "was developed to encourage and enhance cardholder data security" by providing "a baseline of technical and operational requirements designed to protect account data."[22] PCI DSS sets the minimum level of what must be done, not the maximum.

65. PCI DSS 3.2 imposes the following requirements on Defendant:[23]

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

[21] Payment Card Industry Data Security Standard v3.2, at 5 (April 2016) *available at* https://www.pcihispano.com/contenido/uploads/2016/09/PCI_DSS_v3-2-1.pdf

[22] *Id.*

[23] *Id.*

66. Among other things, PCI DSS required Defendant to properly secure and protect payment card data; not store cardholder data beyond the time necessary to authorize a transaction; maintain up-to-date antivirus software and a proper firewall; protect systems against malware; establish a process to identify and timely fix security vulnerabilities; and encrypt payment card data at the point of sale.

67. PCI DSS also required Defendant not to store "the full contents of…the magnetic stripe located on the back of a card" or "the card verification code or value" after authorization.[24] Despite understanding the consequences of inadequate data security, Defendant failed to comply with PCI DSS requirements and failed to take additional protective measures beyond those required by PCI DSS.

F. Defendant Failed to Comply with Federal and State Requirements

68. Federal and State governments have likewise established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions.

69. There are a number of state and federal laws and requirements and industry standards governing the protection of payment card data.

70. For example, at least 24 states have enacted laws addressing data security practices that require that businesses that own, license or maintain personal information about a resident of that state to implement and maintain "reasonable security procedures and practices" and to protect personal information from unauthorized access. California is one such state and, per the California Consumer Privacy Act, requires that "A business that owns, license, or maintains personal information about a California resident shall implement and maintain reasonable security procedures appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use

[24] *Id.* at 38 (PCI DSS 3.2.1 and 3.2.2).

modification or disclosure." Cal. Civ. Code § 1798.81.5(b). Personal information under these statutes usually is defined to include an individual's first name or initial and last name in combination with a credit or debit card number that is in combination with any required security code, access code, or password that would permit access to the individual's financial account. See, e.g., Cal. Civ. Code § 1798.81.5(d)(1)(A)(iii).

71. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[25]

72. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[26] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

73. The FTC recommends that companies not maintain cardholder information longer than is needed for authorization of a transaction; limit access

[25] Federal Trade Commission, *Start With Security*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

[26] Federal Trade Commission, *Protecting Personal Information*: *A Guide for Business*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[27]

74. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

75. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

76. In this case, Defendant was at all times fully aware of its obligation to protect the PII of customers because of its participation in payment card processing networks. Defendant was also aware of the significant repercussions if it failed to do so because Defendant collected payment card data from tens of thousands of customers daily and they knew that this data, if hacked, would result in injury to consumers, including Plaintiff and Class members.

77. Despite understanding the consequences of inadequate data security, Defendant operated POS systems with the outdated magstripe method; failed to enable point-to-point and end-to-end encryption and failed to take other measures necessary to protect its data network.

G. Plaintiff and Class Members Are Damaged

78. The PII of Plaintiff and Class members is private and sensitive in nature and was left inadequately protected by Defendant. Defendant did not obtain

[27] Federal Trade Commission, *supra* note 26.

Plaintiff's and Class members' consent to disclose PII to any other person as required by applicable law and industry standards.

79. Defendant also failed to notify Plaintiff and Class Members of the Data Breach, in direct violation of data breach notification laws, such as California Civil Code § 1798.82.

80. The Data Breach was a direct and proximate result of Defendant's failure to properly safeguard and protect Plaintiff's and Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Defendant's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

81. Had Defendant remedied the deficiencies in its POS systems, followed PCI DSS guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented intrusion into its POS systems and, ultimately, the theft of customers' PII.

82. As a result of Defendant's wrongful actions, inaction, negligent security practices, and the resulting Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured.

83. Defendant's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. unauthorized charges on debit and credit card accounts;

b. theft of personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts;

d. damages arising from the inability to use debit or credit card accounts because accounts were suspended or otherwise rendered unusable as a result of fraudulent charges stemming from the Data Breach;

e. damages arising from the inability to withdraw or otherwise access funds because accounts were suspended, restricted, or otherwise rendered unusable as a result of the Data Breach, including, but not limited to, missed bill and loan payments, late-payment charges, and lowered credit scores and other adverse impacts on credit;

f. costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, including, but not limited to, lost productivity and opportunity(ies), time taken from the enjoyment of one's life, and the inconvenience, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

g. imminent and impending injury resulting from the potential fraud and identity theft posed by PII being exposed for theft and sale on the dark web;

h. loss of use of, and access to, their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and

i. the loss of Plaintiff's and Class members' privacy.

84. While Plaintiff's and Class members' PII has been stolen, Defendant continues to hold PII of consumers, including Plaintiff and Class members. Because Defendant has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and Class members have a strong interest in ensuring that their PII is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

CLASS ACTION ALLEGATIONS

85. Plaintiff brings this lawsuit as a class action on behalf of himself and all others similarly situated as members of the proposed classes pursuant to Federal Rules of Civil Procedure 23(a) and 23(b)(3):

A. The Nationwide Class

86. Plaintiff seeks to represent a class comprised of United States residents (the "Nationwide Class"), defined as follows:

> All persons residing in the United States who made a credit or debit card purchase at any affected Dickey's Barbecue Pit restaurant during the period of the Data Breach.

B. The California Subclass

87. Plaintiff seeks to represent a class comprised of California residents (the "California Subclass"), defined as follows:

> All persons residing in the State of California who made a credit or debit card purchase at any affected Dickey's Barbecue Pit restaurant during the period of the Data Breach.

88. Collectively, the Nationwide Class and California Subclass will be referred to as "the Class" except where there is need to distinguish the class and subclass.

89. Excluded from the proposed Class are Defendant, including any entity in which Defendant has a controlling interest, is a subsidiary, or which is controlled by Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant.

90. Plaintiff reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

91. **Numerosity**: Although the exact number of Class members is uncertain and can only be ascertained through appropriate discovery, the number is great enough – with the Data Breach impacting approximately 3 million customer accounts - such that joinder is impracticable. The disposition of the claims of these Class members in a single action will provide substantial benefits to all parties and to the Court. The Class members may be identifiable from objective means, such as information and records in Defendant's possession, custody, or control.

92. **Commonality and Predominance**. Common questions of law and fact exist as to the proposed Class members and predominate over questions affecting only individual Class members. These common questions include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant's security measures to protect their POS systems were reasonable in light of the PCI DSS requirements, FTC data security recommendations, and best practices recommended by data security experts;

c. Whether Defendant's failure to implement adequate data security measures resulted in or was the proximate cause of the breach of its POS

data systems;

d. Whether Defendant's conduct, including their failure to act, resulted in or was the proximate cause of the breach of the POS systems, resulting in the loss of PII of Plaintiff and Class members;

e. Whether Defendant owed a legal duty to Plaintiff and the other Class members to exercise due care in collecting, storing, and safeguarding their PII;

f. Whether Defendant negligently or recklessly breached legal duties owed to Plaintiff and the other Class members to exercise due care in collecting, storing, and safeguarding their PII;

g. Whether Plaintiff and the Class are at an increased risk for identity theft because of the Data Breach;

h. Whether Defendant's conduct violated Cal. Bus. & Prof. Code § 17200, et seq.;

i. Whether Defendant violated section 1798.150 of the California Consumer Privacy Act by failing to prevent Plaintiff's and Class members' nonencrypted and nonredacted PII from unauthorized access and exfiltration, theft, or disclosure, as a result of Defendant's violations of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information;

j. Whether Plaintiff and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

k. Whether Plaintiff and the other Class members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

93. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the other Class members. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

94. **Typicality**: Plaintiff's claims are typical of the claims of the members of the Classes. Plaintiff is a consumer who used his payment card at an affected Dickey's restaurant locations and had his payment card data compromised as a result of the Data Breach. Plaintiff's damages and injuries are akin to other Class members, and Plaintiff seeks relief consistent with the relief of the Class members.

95. **Adequacy of Representation**: Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the other Class members he seeks to represent; he has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and Plaintiff's counsel.

96. **Superiority**: A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

97. Plaintiff incorporates by reference all allegations in this Complaint as though fully set forth herein.

98. Defendant solicited and took possession of Plaintiff's and the Class members' PII, and Defendant had a duty to exercise reasonable care in securing that information from unauthorized access or disclosure. Defendant also had a duty to timely notify Plaintiff and the Class that their PII had been or may have been stolen. Defendant further had a duty to destroy Plaintiff's and Class members' PII within an appropriate amount of time after it was no longer required by Defendant, in order to mitigate the risk of such non-essential PII being compromised in a data breach.

99. Upon accepting and storing Plaintiff's and Class members' PII in its computer systems and on its networks, Defendant undertook and owed a duty of care to Plaintiff and Class members to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII and to use commercially-reasonable methods to do so. Defendant knew that the PII was private and confidential and should be protected as private and confidential.

100. Defendant owed a duty of care to not subject Plaintiff and Class members, along with their PII, to an unreasonable risk of harm because they were foreseeable and probable victims of inadequate security practices.

101. Defendant owed a duty of care to Plaintiff and Class members to quickly detect a data breach and to timely act on warnings about data breaches.

102. Defendant's duties arose from its relationship to Plaintiff and Class members and from industry custom.

103. Defendant, through its actions and/or failures to act, unlawfully breached duties to Plaintiff and Class members by failing to implement standard

industry protocols and to exercise reasonable care to secure and keep private the PII entrusted to it.

104. Defendant, through its actions and/or failures to act, allowed unmonitored and unrestricted access to its customers' unsecured PII.

105. Defendant, through its actions and/or failures to act, failed to provide adequate supervision and oversight of the PII with which it was entrusted, despite knowing the risk and foreseeable likelihood of a breach and misuse, which permitted unknown third parties to gather Plaintiff's and Class members' PII, misuse that PII, and intentionally disclose it to unauthorized third parties without consent.

106. Defendant knew, or should have known, the risks inherent in collecting and storing PII, the vulnerabilities of POS systems, and the importance of adequate security. Defendant was aware, or should have been aware, of numerous, well-publicized data breaches within the restaurant industry.

107. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class members' PII.

108. Due to Defendant's knowledge that a breach of its systems could damage millions of its customers, including Plaintiff and Class members, Defendant had a duty to adequately protect its data systems and the PII contained therein.

109. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their PII. Defendant's misconduct included failing to: (1) secure the POS systems, despite knowing its vulnerabilities; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

110. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiff's and Class members' PII, and promptly notify them about the Data Breach.

111. Defendant breached its duties to Plaintiff and Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PII;

b. by creating a foreseeable risk of harm through the misconduct previously described;

c. by failing to comply with industry standard data security standards during the period of the Data Breach; and

d. by failing to timely and accurately disclose that Plaintiff's and Class members' PII had been improperly acquired or accessed.

112. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect Plaintiff's and Class members' PII from being foreseeably captured, accessed, disseminated, stolen, and misused, Defendant unlawfully breached its duties to use reasonable care to adequately protect and secure Plaintiff's and Class members' PII while it was within Defendant's possession or control.

113. Upon information and belief, Defendant improperly and inadequately safeguarded Plaintiff's and Class members' PII in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Defendant's failure to take proper security measures to protect customers' PII as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiff's and Class members' PII.

114. In engaging in the negligent acts and omissions as alleged herein, which permitted an unknown third party to access Defendant's customers' PII,

Defendant violated Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce." This prohibition includes failing to have adequate data security measures and failing to protect their customers' PII.

115. Plaintiff and the Class members are among the class of persons Section 5 of the FTC Act was designed to protect, and the injuries suffered by Plaintiff and the Class members is the type of injury Section 5 of the FTC Act was intended to prevent. As a result, Defendant is negligent per se.

116. Neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint.

117. Defendant's failure to exercise reasonable care in safeguarding PII by adopting appropriate security measures was the direct and proximate cause of Plaintiff's and Class members' PII being accessed and stolen through the data breach.

118. Defendant breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PII.

119. As a result of Defendant's breach of its duties, Plaintiff and the Class members suffered or are at increased risk of suffering damages including, but not limited to: loss of right to privacy of PII, damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of their PII; damages arising from Plaintiff's and Class members' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying

financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT II
Violations of California's Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq.*
(On Behalf of Plaintiff and the Nationwide Class)

120. Plaintiff incorporates by reference all allegations in this Complaint as though fully set forth herein.

121. Defendant's business practices as complained of herein violate the Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*. ("UCL").

122. Defendant's practices constitute "unlawful" business practices in violation of the UCL because, among other things, they violate statutory law and the common law, including without limitation the California Consumer Privacy Act, Cal. Civ. Code § 1798.150 and Section 5 of the FTC Act.

123. Defendant's actions and practices constitute "unfair" business practices in violation of the UCL, because, among other things, the gravity of the harm to Plaintiff and the Class members outweighs the utility of Defendant's conduct. This conduct includes Defendant's failure to adequately ensure the privacy, confidentiality, and security of customers' data entrusted to it and Defendant's failure to have adequate data security measures in place.

124. As a result of Defendant's wrongful business practices, Plaintiff and members of the Class have suffered injury in fact and lost money or property as alleged herein.

125. Defendant's wrongful business practices present an ongoing and continuing threat to the general public.

126. Accordingly, Plaintiff and Class members have and will incur economic damages related to the breach including, time and money spent remedying the breach, monitoring their financial accounts to ensure no further fraud or no fraud is perpetuated; time spent insuring that any unauthorized charges are identified and remedied; experiencing lack of access to funds while banks and financial institutions issue new cards; and the costs of credit monitoring, purchasing credit reports, and purchasing "freezes" to prevent opening of unauthorized accounts.

COUNT III
Violation of the California Consumer Privacy Act
Cal. Civ. Code § 1798.150
(On Behalf of Plaintiff and the California Subclass)

127. Plaintiff incorporates by reference all allegations in this Complaint as though fully set forth herein.

128. Defendant collects consumers' personal information as defined in Cal. Civ. Code § 1798.140. As a result, Defendant has a duty to implement and maintain reasonable security procedures and practices to protect this personal information. As alleged herein, Defendant failed to do so.

129. Defendant violated § 1798.150 of the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiff and Class members' nonencrypted and nonredacted PII from unauthorized access and exfiltration, theft, or disclosure. These failures were the result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

130. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class members' PII, including names, payment card numbers, payment card expiration dates, and payment card security codes, was subjected to unauthorized

access, exfiltration, and theft. On information and belief, Plaintiff and the Class allege this PII was not encrypted or redacted in the format accessed during the Data Breach.

131. Plaintiff and the Class members seek injunctive or other equitable relief to ensure Defendant hereafter adequately safeguards customers' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold customers' PII, including that of Plaintiff and the California Subclass. These individuals have an interest in ensuring that their PII is reasonably protected.

132. On April 5, 2021, Plaintiff's Counsel sent a notice letter to Defendant Dickey's Barbecue Restaurants, Inc.'s registered service agent via FedEx Priority. Assuming Defendant cannot cure the Data Breach within 30 days, and Plaintiff believes any such cure is not possible under these facts and circumstances, Plaintiff intends to promptly amend this complaint to seek actual damages and statutory damages of no less than $100 and up to $750 per customer record subject to the Data Breach on behalf of the California Subclass as authorized by the CCPA.

COUNT IV
Declaratory Judgment
(On Behalf of Plaintiff and the California Subclass)

133. Plaintiff incorporates by reference all allegations in this Complaint as though fully set forth herein.

134. There exists a controversy regarding the reasonableness of the security measures Defendant provided as applicable to Plaintiff's claim under the CCPA.

135. A judicial determination addressing the issues is necessary now to avoid additional data breaches due to insufficient security protection.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly

situated, respectfully requests that the Court enter an order:

a. Certifying the proposed Class as requested herein;

b. Appointing Plaintiff as Class Representative and undersigned counsel as Class Counsel;

c. Finding that Defendant engaged in the unlawful conduct as alleged herein;

d. Enjoining Defendant's conduct and requiring Defendant to implement proper data security policies and practices;

e. Awarding Plaintiff and Class members damages;

f. Awarding Plaintiff and Class members pre-judgment and post-judgment interest on all amounts awarded;

g. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and expenses; and

h. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the proposed Class, hereby demands a trial by jury as to all matters so triable.

Dated: April 5, 2021

/s/ Gayle M. Blatt
GAYLE M. BLATT

CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP

Attorneys for Plaintiff and the putative Classes