IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

DEMI KOSTKA, individually and on behalf of all others similarly situated, Plaintiff, v. DICKEY'S BARBECUE RESTAURANTS, INC., Defendant.	)	CASE NO. 3:20-cv-3424 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

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

NATURE OF THE ACTION

1. Plaintiff brings this action, individually and on behalf of all others similarly situated whose private and confidential financial information, including credit card and debit card numbers, expiration dates, cardholder names, internal card verification codes, and other payment card information (collectively, "Card Information") was compromised in a massive security breach of Dickey's computer servers and payment card environment (the "Data Breach").

2. As a result of the Data Breach, leading cybersecurity expert Krebs on Security ("Krebs") reports that highly sensitive consumer card information for an estimated 3 million

payment cards used at Dickey's restaurant locations during the Data Breach are available for purchase on the notorious dark web commerce site Joker's Stash.[1] As a result of the Data Breach, Plaintiff and these similarly situated consumers have had their highly sensitive Card Information exposed to criminals.

3. An initial statement offered by Dickey's on October 15 contained very little detail about the Data Breach. The company merely identified:

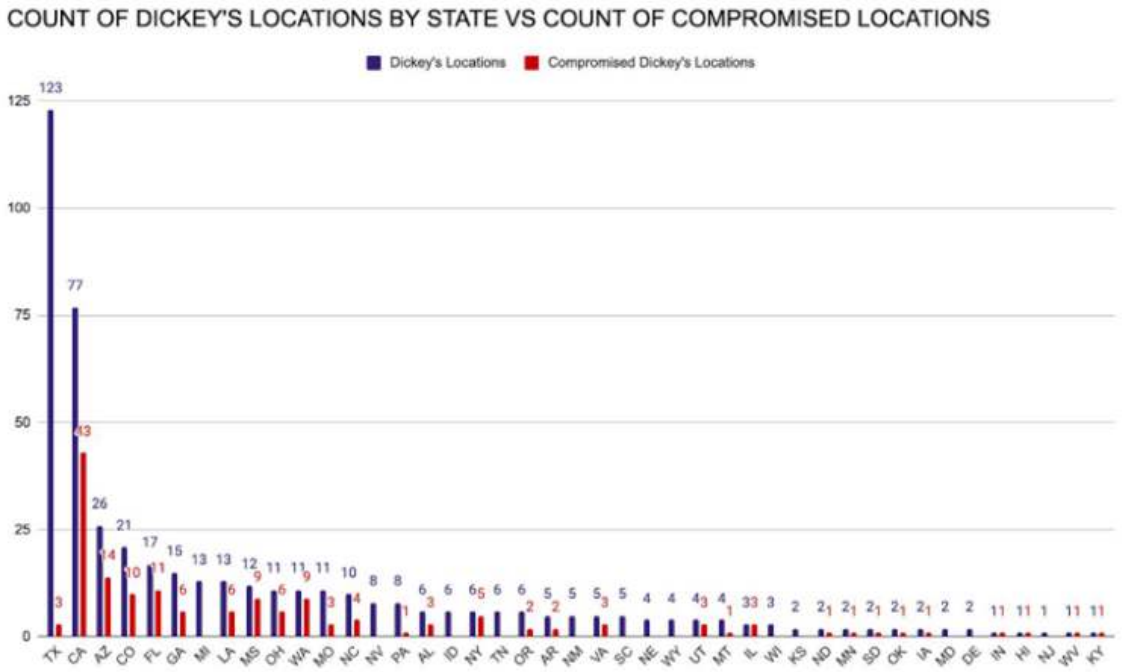
> We received a report indicating that a payment card security incident may have occurred. We are taking this incident very seriously and immediately initiated our response protocol and an investigation is underway. We are currently focused on determining the locations affected and time frames involved. 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.[2]

4. Early reports from leading cyber intelligence firms Gemini Advisory and Q6Cyber indicate that the breach is massive in scope and duration. Gemini indicated that 156 Dickey's locations across 30 states likely had payment systems compromised, and that the window of exposure is 13 months, from July 2019 to August 2020.[3] Q6Cyber's report identified that the window may be even longer, from May 2019 through September 2020, or 17 months.[4]

---

[1] *Breach at Dickey's BBQ Smokes 3M Cards*, KREBSONSECURITY (Oct. 20, 2020), https://krebsonsecurity.com/2020/10/breach-at-dickeys-bbq-smokes-3m-cards/.
[2] *Id.*
[3] *Id.*
[4] *Id.*

5. While no reports have issued from Dickey's yet confirming the window or magnitude of the Data Breach, a recent ZDNet article has tallied the total number of locations, by state, identified as being impacted by the Data Breach in the chart below[5]:



6. As alleged herein, Dickey's' failure to implement adequate data security measures to protect its customers' sensitive Card Information directly and proximately caused injuries to Plaintiff and class members.

7. The Data Breach was the inevitable result of Dickey's' inadequate data security measures and cavalier approach to data security. Despite the well-publicized and ever-growing threat of security breaches involving payment card networks and systems, and even though these types of data breaches were and are occurring frequently throughout the restaurant and retail

[5] Catalin Cimpanu, *Card details for 3 million Dickey's customers posted on carding forum*, ZDNET (Oct. 15, 2020), https://www.zdnet.com/article/card-details-for-3-million-dickeys-customers-posted-on-carding-forum/.

industries, Dickey's failed to ensure that it maintained adequate data security measures to protect customer Card Information from criminals.

8. As a direct and proximate result of Dickey's cavalier conduct and data security negligence, a massive amount of customer information was stolen from Dickey's and exposed to criminals. Victims of the Data Breach have had their sensitive Card Information compromised, had their privacy rights violated, face an increased risk of fraud and identify theft, lost control over their personal and financial information, and otherwise have been injured.

9. Moreover, Plaintiff and class members have been forced to spend significant time associated with, among other things, closing out and opening new credit or debit card accounts, ordering replacement cards, obtaining fraud monitoring services, losing access to cash flow and credit lines, monitoring credit reports and accounts, purchasing identity theft insurance, and/or other losses resulting from the unauthorized use of their cards or accounts.

10. Dickey's has not offered meaningful assistance to consumers to help deal with the fraud that has and will continue to result from the Data Breach. In contrast to what has been frequently made available to consumers in other data breaches, Dickey's has not offered or provided any credit monitoring service or fraud insurance to date, and has failed to provide Plaintiff and class members with notice of the breach

11. Plaintiff and class members seek to recover damages caused by Dickey's negligence, negligence per se, breach of implied contract, and unjust enrichment. Additionally, Plaintiff seeks declaratory and injunctive relief as a result of the conduct of Dickey's discussed herein.

I. PARTIES

A. Plaintiff Demi Kostka

12. Plaintiff Demi Kostka is an adult citizen of Florida, residing in Gulf Breeze, Santa Rosa County, Florida.

B. Defendant Dickey's Barbecue Restaurants, Inc.

13. Defendant Dickey's, Barbecue Restaurants, Inc. is corporation that is incorporated in Texas and maintains its principal place of business at 18583 North Dallas Pkwy, Suite 120, Dallas, Texas 75287. It can be served through its registered agent for service: C T Corporation System, 1999 Bryan St., Ste. 900, Dallas, TX 75201-3136.

14. Dickey's is a family-owned franchise that operates smoked-meat and barbecue restaurant locations called Dickey's Barbecue Pit. The restaurant franchise has 469 locations across 42 states, including, notably, 123 locations in Texas, 77 locations in California, 26 locations in Arizona, and 21 locations in Colorado.

II. JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5 million, exclusive of interest and costs, and is a class action in which some members of the class are citizens of states different than Dickey's. *See* 28 U.S.C. § 1332(d)(2)(A).

16. This Court has general personal jurisdiction over Dickey's. Dickey's has systematic and continuous contacts with the state of Texas. Dickey's is a Texas corporation and maintains its principal place of business in Texas. Dickies also operates over 100 Dickey's locations in Texas and conducts substantial business within this judicial district.

17. Venue properly lies in this district pursuant to 28 U.S.C. § 1391(b) because Dickey's has corporate headquarters in this district and is thus deemed to reside in this district;

Dickey's conducts substantial business in this district; and a substantial part of the events and/or omissions giving rise to the claims occurred, in part, within this district.

III. FACTUAL ALLEGATIONS

18. On August 10, 2020, during the window of the Data Breach, Ms. Kostka used her Wells Fargo debit card to make a $43.61 purchase at the Dickey's location at 1480 Tiger Park Lane, Gulf Breeze, Florida.

19. On November 13, 2020, Ms. Kostka discovered that a criminal had used her Wells Fargo debit card information to make an unauthorized $24.95 purchase in South Hackensack, New Jersey. Ms. Kostka suffered actual, palpable fraud due to the Data Breach. Prior to experiencing this fraud, Ms. Kostka never suffered fraud on her Wells Fargo debit card, and she never received notice that she had been impacted by another data breach impacting her debit card.

20. After discovering the fraudulent charge, Ms. Kostka turned off her debit card and called Wells Fargo to file a claim regarding the fraud on her debit card. Wells Fargo immediately cancelled Ms. Kostka's debit card upon being advised of the fraudulent activity. Ms. Kostka is currently without the ability to use her debit card, which is the main bank account she uses to pay day-to-day expenses.

21. To date Ms. Kostka is still waiting for a replacement debit card, and does not have immediate access to her Wells Fargo debit card account and funds.

22. Dickey's has not provided direct notice of the Data Breach to Ms. Kostka.

23. As a result of being victimized by the Data Breach, Ms. Kostka was also required to spend a significant amount of time addressing fraud concerns related to her compromised

card. To date, Ms. Kostka has spent 3 to 4 hours of time calling her bank and continuously monitoring her accounts for fraudulent activity.

24. Had Ms. Kostka known that Dickey's would not adequately protect her Card Information and other sensitive information entrusted to it, she would not have made a purchase at Dickey's using her payment card.

25. As a result of Dickey's' failure to adequately safeguard Plaintiff Kostka's Card Information, she has been injured

A. The Dickey's Data Breach

26. Dickey's Barbecue Pit, the largest barbecue restaurant chain in the United States, suffered a massive data breach between July 2019 and August 2020.

27. The Dallas-based franchise has 469 locations (411 of which are currently open during the pandemic) across 42 states.

28. Dickey's reportedly was alerted about the breach days before on October 13, 2020 by Krebs.[6]

29. According to Krebs, credit card and debit card information for more than 3 million of Dickey's customers is now being sold on the dark web—an underground part of the internet accessed by an anonymizing browser and that is not indexed by search engines, where rampant illegal commerce occurs (e.g., buying and selling stolen card, subscription, and account information/credentials; buying and selling drugs, guns, counterfeit money). The card data stolen during the Data Breach is reportedly being offered for sale on a well-known website called

[6] *Id*.

Joker's Stash, where the cache of stolen, for-purchase payment card information is listed as the "BlazingSun" breach, with card data available for $17 apiece.[7]

30. Multiple companies that track the sale in stolen payment card data say that they have confirmed with card-issuing financial institutions that the accounts for sale in the BlazingSun batch have one common theme: all of them were used at various Dickey's BBQ locations over the past 13 to 15 months.[8]

31. Although Dickey's has not confirmed whether the Data Breach exposed credit and debit card numbers, cardholder names, and card expiration dates, the cache of data available for sale on Joker's Stash makes clear that this level of information involving customers' credit and debit card information was certainly stolen from Dickey's as part of the Data Breach.

32. Dickey's has also not confirmed the scope or magnitude of the breach, but early reports from leading cyber intelligence firms Gemini Advisory and Q6Cyber indicate that 156 Dickey's locations across 30 states likely had payment systems compromised. While Gemini reports that the window of exposure is 13 months, from July 2019 to August 2020, Q6 separately reported that the breach window may be as long as 17 months, from May 2019 to September 2020.[9]

33. As is typical with payment card data breaches, the Data Breach was most likely the result of malware that criminals routinely use in payment card breaches. According to the Krebs report, "Gemini says its data indicated some 156 Dickey's locations across 30 states likely

[7] *Id.*
[8] *Id.*
[9] *Id.*

had payment systems compromised by card-stealing malware, with the highest exposure in California and Arizona."[10]

34. Gemini further indicated:

> Dickey's operates on a franchise model, which often allows each location to dictate the type of point-of-sale (POS) device and processors that they utilize . . . However, given the widespread nature of the breach, the exposure may be linked to a breach of the single central processor, which was leveraged by over a quarter of all Dickey's locations.[11]

35. According to Gemini Advisory researchers, based on previous major breaches uploaded to Joker's Stash, the records from Dickey's Barbecue Pit will likely continue to be added to this marketplace over the next several months.[12]

36. Q6Cyber's CEO Eli Dominitz identified that "[t]he financial institutions we've been working with have already seen a significant amount of fraud related to these cards."[13]

37. No statements or press issued by Dickey's to date give any indication as to the actual magnitude of the Data Breach, including confirmation of the number of stores impacted or the actual number of customers and cards affected. Dickey's has provided virtually no details surrounding the breach that would allow consumers to protect themselves against payment card fraud and identity theft.

38. Warren Poschman, senior solutions architect with data-security company Comforte AG, says that store merchants like Dickey's need to require the use of secure connections—from the point-of-sale device to the backend—using point-to-point encryption

---

[10] *Id*.
[11] *Id*.
[12] Lindsey O'Donnell, *Dickey's BBQ Breach: Meaty 3M Payment Card upload Drops on Joker's Stash*, threatpost (Oct. 16, 2020), https://threatpost.com/dickeys-bbq-breach-jokers-stash/160211/.
[13] *Breach at Dickey's BBQ Smokes 3M Cards*, KREBSONSECURITY *supra* note 1.

tokenization. Mr. Poschman further stressed that backend payment processors (and the merchants that outsource to them) must also tokenize all data to ensure that any breach will not result in exposure.[14]

39. According to Poschman, the Dickey's BBQ Data Breach reminds us that "there is still plenty of meat on the bone of credit card fraud despite the dramatic shift in coverage to privacy and identity theft." And the pandemic is no excuse for negligent security safeguards, says Poschman: "With COVID-19 pushing businesses in the fast-casual restaurant segment to the brink, attackers are taking advantage of lax security while many are in survival mode. Regardless of the ill timing, organizations need to ensure that every step in the payment cycle is secured from acquisition to settlement."[15]

B. Industry Standards and the Protection of Customer Card Information

40. It is well known in the retail industry that sensitive Card Information is valuable and frequently targeted by hackers. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers. . . . Many of them were caused by flaws in payment systems either online or in stores."[16]

41. Despite the known risk of POS malware intrusions and the widespread publicity and industry alerts regarding other notable (similar) data breaches, Dickey's failed to take reasonable steps to adequately protect its computer systems and payment card environment from being breached, and then failed to detect the Data Breach for many months.

---

[14] Lindsey O'Donnell, *supra* note 14.
[15] *Id.*
[16] Dennis Green and Mary Hanbury, *If you bought anything from these 11 companies in the last year, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

42. Dickey's is, and at all relevant times has been, aware that the Card Information it maintains as a result of purchases made at its locations is highly sensitive and could be used for nefarious purposes by third parties.

43. Dickey's' explicit statements in its Privacy Policy make clear that Dickey's recognized the importance of adequately safeguarding its customers' sensitive Card Information yet failed to take the steps necessary to protect that sensitive data. On its website, Dickey's' Privacy notice provides the following:

> **Dickey's Commitment to Privacy:**
>
> At Dickey's Barbecue Restaurants, Inc. ("Dickey's"), we understand that our customers are concerned about the use of their personal information, and we respect our customer's privacy. This Privacy Policy explains the steps we have taken to ensure that the personal information you submit to us is secure and kept confidential.[17]

44. Dickey's is thus aware of the importance of safeguarding its customers' Card Information from the foreseeable consequences that would occur if its data security systems and computer servers were breached.

45. Financial institutions and credit card processing companies have issued rules and standards governing the basic measures that merchants must take to ensure that consumers' valuable data is protected.

46. The Payment Card Industry Data Security Standard ("PCI DSS") is a list of twelve information security requirements that were promulgated by the Payment Card Industry Security Standards Council. The PCI DSS list applies to all organizations and environments where cardholder data is stored, processed, or transmitted, and requires merchants like Dickey's to protect cardholder data, ensure the maintenance of vulnerability management programs,

[17] *Privacy Policy,* DICKEY'S BARBECUE PIT, https://cms-www-dickeys-com-development.s3.amazonaws.com/privacy_policy_4cb941a12c.pdf (last visited Oct. 20, 2020).

implement strong access control measures, regularly monitor and test networks, and ensure the maintenance of information security policies.

47. The twelve requirements of the PCI DSS are: (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; (3) Protect stored cardholder data; (4) Encrypt transmission of cardholder data across open, public networks; (5) Protect all systems against malware and regularly update anti-virus software or programs; (6) Develop and maintain secure systems and applications; (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; (10) Track and monitor all access to network resources and cardholder data; (11) Regularly test security systems and processes; (12) Maintain a policy that addresses information security for all personnel.[18]

48. Furthermore, PCI DSS sets forth detailed and comprehensive requirements that must be followed to meet each of the twelve mandates.

49. Dickey's was, at all material times, fully aware of its data protection obligations in light of its participation in the payment card processing networks and its daily collection and transmission of thousands of sets of Card Information.

50. Because Dickey's accepted payment cards containing sensitive financial information, it knew that its customers were entitled to and did in fact rely on it to keep that

[18] *PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard Version 3.2*, PCI SECURITY STANDARDS COUNCIL (May 2016), https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_2.pdf?agreement=true&time=1506536983345.

sensitive information secure from would-be data thieves in accordance with the PCI DSS requirements.

51. Additionally, according to the Federal Trade Commission ("FTC"), the 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 Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 248 (3d Cir. 2015); *see also See Consumer Data Protection: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce*, 2011 WL 2358081, at *6 (June 15, 2011) (statement of Edith Ramirez, Comm'r, FTC) ("[T]he Commission enforces the FTC Act's proscription against unfair . . . acts . . . in cases where a business['s] . . . failure to employ reasonable security measures causes or is likely to cause substantial consumer injury."); *Data Theft Issues: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce*, 2011 WL 1971214, at *7 (May 4, 2011) (statement of David C. Vladeck, Director, FTC Bureau of Consumer Protection) (same).

52. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that 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 for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating

someone may be trying 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.

53. The FTC has also published a document, entitled "Protecting Personal Information: A Guide for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[19]

54. The FTC has issued orders against businesses that failed to employ reasonable measures to secure payment card data. These orders provide further guidance to businesses with regards to their data security obligations.

55. Dickey's was aware or should have been aware of FTC guidelines and other guidance regarding data security.

C. Dickey's Disregarded Industry Standards for Customer Data Security

56. Dickey's is no stranger to security breaches. In 2015, Dickey's experienced a ransomware attack with a $6,000 extortion demand,[20] thus Dickey's had a heightened awareness of the risk of security breaches.

57. Despite this, Dickey's failed to upgrade and maintain its data security systems in a meaningful way in order prevent data breaches. Dickey's security flaws run afoul of industry best practices and standards. More specifically, the security practices in place at Dickey's are in stark contrast and directly conflict with the PCI DSS core security standards.

---

[19] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Nov. 2011), https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

[20] https://geminiadvisory.io/jokers-stash-breaches-dickeys/ (last visited Nov. 16, 2020).

58. Had Dickey's maintained its information technology systems ("IT systems"), adequately protected them, and had adequate security safeguards in place, it could have prevented the Data Breach.

59. As a result of FTC and other regulatory guidance, industry warnings, awareness of industry best practices, the PCI DSS, and numerous well-documented restaurant and retail (and other) data breaches, Dickey's was alerted to the risk associated with failing to ensure that its computer and payment card systems were adequately secured.

60. Dickey's was not only aware of the threat of data breaches, generally, but was aware of the specific danger of malware infiltration. Malware has been used recently to infiltrate large retailers such as, *inter alia*, Wawa, Hy-Vee, Target, Sonic, GameStop, Chipotle, Jason's Deli, Whole Foods, Sally Beauty, Neiman Marcus, Michaels Stores, and Supervalu. As a result, Dickey's was aware that malware is a real threat and is a primary tool of infiltration used by hackers seeking to carry out payment card breaches.

61. In addition to the publicly announced data breaches described above (among many others), Dickey's knew or should have known of additional warnings regarding malware infiltrations from the U.S. Computer Emergency Readiness Team, a government unit within the Department of Homeland Security, which alerted retailers to the threat of malware on July 31, 2014, and issued a guide for retailers on protecting against the threat of malware, which was updated on August 27, 2014.[21]

62. Despite the fact that Dickey's was on notice of the very real possibility of consumer data theft associated with its security practices and that Dickey's knew or should have

[21] *See Alert (TA14-212A): Backoff Point-of-Sale Malware*, U.S. COMPUTER EMERGENCY READINESS TEAM (July 31, 2014) (revised Sept. 30, 2016), https://www.us-cert.gov/ncas/alerts/TA14-212A.

known about the elementary infirmities associated with its security systems, it still failed to make necessary changes to its security practices and protocols, and permitted massive malware intrusions to occur for months on end.

63. Dickey's, at all times relevant to this action, had a duty to Plaintiff and members of the class to: (a) properly secure Card Information submitted to or collected at Dickey's locations and on Dickey's internal networks; (b) encrypt Card Information using industry standard methods; (c) use available technology to defend its systems from well-known methods of invasion; (d) act reasonably to prevent the foreseeable harms to Plaintiff and class members, which would naturally result from Card Information theft; and (e) promptly notify customers when Dickey's became aware of the potential that customers' Card Information may have been compromised.

64. Dickey's permitted customers' Card Information to be compromised by failing to take reasonable steps against an obvious threat.

65. In addition, leading up to the Data Breach, during the breach itself, and during the investigation that followed, Dickey's failed to follow the guidelines set forth by the FTC.

66. Industry experts are clear that a data breach is indicative of data security failures. Indeed, industry-leading research and advisory firm Aite Group has identified that: "If your data was stolen through a data breach that means you were somewhere out of compliance" with payment industry data security standards.[22]

67. The Data Breach is particularly egregious and its data security failures are particularly alarming given that the breach reportedly resulted in at least 3 million cards being

[22] Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May 26, 2017), http://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY.

stolen and illegally placed for sale on the dark web, and because the Data Breach was permitted to occur for over 13 months at 156 locations. Clearly, had Dickey's utilized adequate data security and data breach precautions, the window of the Data Breach would have been significantly mitigated, and the level of impact could have been reduced, had the breach been permitted to happen at all in the first place.

68. One commentator in the data security industry noted as to a previous, unrelated data breach:

> 2 million cards on sale on the dark web would indicate this was a very successful project for the cybercriminals involved, and one which is likely to be incredibly profitable. POS-malware breaches happen in the US with alarming regularity, and businesses should be well aware that they need to not only protect their central networks but also need to account for physical locations as well. . . . Moving forward, financial institutions should consider implementing a system of two-factor authentication in conjunction with a passive biometric solutions in order to mitigate the entirely avoidable outcomes of security incidents such as this.[23]

69. With more than 3 million cards reportedly stolen in the Dickey's breach, this clearly marks a highly successful outing for criminals and a large failure on Dickey's part as to data security.

70. As for the criminals purchasing the card data stolen in the Data Breach, they are also reportedly enjoying high levels of success with making fraudulent purchases. An article from the data privacy and cyber security internet newsgroup CPO Magazine indicates that Joker's Stash "is advertising a 'valid rate' of 90 to 100%, indicating that Dickey's has only just

[23] *Cyber Attack on Earl Enterprises (Planet Hollywood)*, isBuzznews (Apr. 1, 2019), https://www.informationsecuritybuzz.com/expert-comments/cyber-attack-on-earl-enterprises-planet-hollywood/.

become aware of the breach." In other words, Joker's Stash is currently promising purchasers of stolen Dickey's payment card data "that at least 90% of them [are] functional."[24]

71. Because payment card data breaches involving malware are so common, and given the high level of data security measures available to companies that take customer payment information in, like Dickey's, there is no reason why Dickey's could not have adequately protected its systems and servers from the Data Breach.

72. As a result of the events detailed herein, Plaintiff and class members suffered actual, palpable fraud and losses resulting from the Data Breach, including: financial losses related to the purchases made at Dickey's that Plaintiff and class members would not have made had they known of Dickey's careless approach to cybersecurity; lost control over the value of personal information; unreimbursed losses relating to fraudulent charges; losses and fees relating to exceeding credit and debit card limits, balances, and bounced transactions; harm resulting from damaged credit scores and information; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Card Information.

73. These costs and expenses will continue to accrue as additional fraud alerts and fraudulent charges occur and are discovered.

[24] Scott Ikeda, *Three Million Credit Cards Harvested and Sold on Joker's Stash; Dickey's BBQ Hack Undetected for Over a Year*, CPO MAGAZINE (Oct. 19, 2020), https://www.cpomagazine.com/cyber-security/three-million-credit-cards-harvested-and-sold-on-jokers-stash-dickeys-bbq-hack-undetected-for-over-a-year/.

74. Furthermore, the Card Information stolen from Dickey's locations can be used to drain debit card-linked bank accounts, make "clone" credit cards, or to buy items on certain less-secure websites.

75. To date, and as made clear in the Krebs Report, Dickey's does not appear to be taking any real measures to assist affected customers. In the first place, it has barely shared any information about the Data Breach, leaving victims of the breach in the dark and vulnerable to continued fraud. All that Dickey's has done to assist impacted customers is to offer this sage advice: "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."[25]

76. These "suggestions" make it clear that Dickey's is shifting the responsibility for the Data Breach to consumers, rather than taking real steps to assist its customers in protecting against the fraud to which Dickey's exposed them. Upon information and belief, to date, Dickey's is not offering credit monitoring or identity theft insurance to customers impacted by the Data Breach.

77. Only now, after the damage from the Data Breach has already occurred, does it appear that Dickey's is taking some steps to attempt to sure up its point of sale ("POS") systems. Indeed, it has published job listings as of November 16, 2020 for POS Implementation Trainer and POS Installer & Support Technician positions on LinkedIn.[26]

---

[25] *See Breach at Dickey's BBQ Smokes 3M Cards*, KREBSONSECURITY, *supra* note 1.

[26] *See* https://www.linkedin.com/jobs/view/2296561058/?alternateChannel=search&refId=w6Zkq53Hiuk0%2BuPHdDEpbw%3D%3D&trackingId=UgN6MGv0nNcQ98JoaNh3Tg%3D%3D&trk=flagship3_search_srp_jobs&lipi=urn%3Ali%3Apage%3Ad_flagship3_search_srp_jobs%3BofaejmspRvqK%2BDrxXQLpbA%3D%3D (last visited Nov. 16, 2020);

78. Dickey's failure to adequately protect its customers' Card Information has resulted in consumers having to undertake various errands (e.g., obtaining credit monitoring, checking credit reports, etc.) that require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of their own money. At the same time, Dickey's is doing nothing to assist those affected by the Data Breach and has withheld important details about the Data Breach as it conducts its investigation. Instead, Dickey's is putting the burden on the consumer to discover possible fraudulent transactions.

IV. CLASS ALLEGATIONS

79. Plaintiff brings this action individually and on behalf of the following class and pursuant to Fed. R. Civ. P. 23:

80. All persons who used a credit card or debit card at a Dickey's location that was impacted by the Data Breach during the period in which Dickey's systems were exposed to the Data Breach.

81. Excluded from the class is Dickey's, its affiliates, officers, directors, assigns, successors, and the Judge(s) assigned to this case. Plaintiff reserves the right to modify, change, or expand the definition of the class based on discovery and further investigation.

82. **Numerosity**: While the precise number of class members has not yet been determined, members of the class are so numerous that their individual joinder is impracticable, as the proposed class appears to include approximately 3 million members who are

---

https://www.linkedin.com/jobs/view/2293333127/?alternateChannel=search&refId=w6Zkq53Hiuk0%2BuPHdDEpbw%3D%3D&trackingId=Dx6SNnzh9C5e9OTC%2FETVEA%3D%3D&trk=flagship3_search_srp_jobs&lipi=urn%3Ali%3Apage%3Ad_flagship3_search_srp_jobs%3BefV8XLTdQOmPgCKr3R8jRw%3D%3D (last visited Nov. 16, 2020).

geographically dispersed. Upon information and belief, the Data Breach affected millions of consumers across the United States.

83. **Typicality**: Plaintiff's claims are typical of class members' claims. Plaintiff and all class members were injured through Dickey's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other class member because Plaintiff and each class member had their sensitive data and Card Information compromised in the same way by the same conduct by Dickey's.

84. **Adequacy**: Plaintiff is an adequate representative of the class because Plaintiff's interests do not conflict with the interests of the class that she seeks to represent; Plaintiff has retained counsel that are competent and highly experienced in class action litigation, including data breach cases in particular; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the class will be fairly and adequately protected by Plaintiff and her counsel.

85. **Superiority**: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the class members. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for class members individually to effectively redress Dickey's wrongdoing. Even if class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far

fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

86. **Existence and Predominance of Common Questions of Fact and Law**: Common questions of law and fact exist as to Plaintiff and all class members. These questions predominate over the questions affecting individual class members. These common legal and factual questions include, but are not limited to, the following:

- whether Dickey's engaged in the wrongful conduct alleged herein;
- whether Dickey's owed duties to Plaintiff and members of the class to protect their Card Information and to provide timely and accurate notice of the Data Breach to Plaintiff and the class, and whether it breached these duties;
- whether Dickey's violated federal and state laws as a result of the Data Breach;
- whether Dickey's knew or should have known that its computer and network systems were vulnerable to attacks from hackers and cyber-criminals;
- whether Dickey's conduct was the proximate cause of the breach of its computer and network systems resulting in the theft of customers' Card Information;
- whether Dickey's wrongfully failed to inform Plaintiff and members of the class that it did not maintain computer software and other security procedures and precautions sufficient to reasonably safeguard consumers' sensitive financial and personal data;
- whether Dickey's failed to inform Plaintiff and the class of the Data Breach in a timely and accurate manner;
- whether Dickey's has taken adequate preventive and precautionary measures to ensure the Plaintiff and class members will not experience further harm;

- whether Plaintiff and members of the class suffered injury as a proximate result of Dickey's conduct or failure to act; and
- whether Plaintiff and the class are entitled to recover damages, equitable relief, and other relief, and the extent of the remedies that should be afforded to Plaintiff and the class.

87. Dickey's has acted or refused to act on grounds generally applicable to Plaintiff and the other members of the class, thereby making appropriate final injunctive relief and declaratory relief with respect to the class as a whole.

88. Given that Dickey's has engaged in a common course of conduct as to Plaintiff and the class, similar or identical injuries and common law and statutory violations are involved, and common questions outweigh any potential individual questions.

89. The class is defined in terms of objective characteristics and common transactional facts; namely, the exposure of sensitive Card Information to cyber criminals due to Dickey's failure to protect this information, adequately warn the class that it lacked adequate data security measures, and failure to adequately warn that it was breached. Class membership will be readily ascertainable from Dickey's business records, and/or from records of third parties.

90. Plaintiff reserves the right to revise the above class definitions and any of the averments of fact herein based on facts adduced in discovery.

V. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

91. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

92. Dickey's collected Card Information from Plaintiff and class members in exchange for its sale of food and other services at its impacted locations.

93. Dickey's owed a duty to Plaintiff and the class to maintain confidentiality and to exercise reasonable care in safeguarding and protecting their financial and personal information in Dickey's possession from being compromised by unauthorized persons. This duty included, among other things, designing, maintaining, and testing Dickey's networks and data security systems to ensure that Plaintiff's and class members' financial and personal information in Dickey's possession was adequately protected in the process of collection and following collection while stored on Dickey's systems.

94. Dickey's further owed a duty to Plaintiff and class members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

95. Dickey's owed a duty to Plaintiff and class members to provide security consistent with industry standards and requirements and to ensure that its computer systems and networks—and the personnel responsible for them—adequately protected the financial and personal information of Plaintiff and class members whose confidential data Dickey's obtained and maintained.

96. Dickey's knew, or should have known, of the risks inherent in collecting and storing Plaintiff's and class members' financial and personal information and the critical importance of providing adequate security for that information.

97. Dickey's conduct created a foreseeable risk of harm to Plaintiff and class members. This conduct included but was not limited to Dickey's failure to take the steps and opportunities to prevent and stop the Data Breach as described herein. Dickey's conduct also

included its decision not to comply with industry standards for the safekeeping and maintenance of the financial and personal information of Plaintiff and class members.

98. Dickey's knew or should have known that it had inadequate computer systems and data security practices to safeguard such information, and Dickey's knew or should have known that hackers would attempt or were attempting to access the personal financial information in databases such as Dickey's.

99. Dickey's breached the duties it owed to Plaintiff and members of the class by failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the medical, financial, and personal information of Plaintiff and members of the class, as identified above. This breach was a proximate cause of injuries and damages suffered by Plaintiff and class members.

100. As a direct and proximate result of Dickey's negligent conduct, Plaintiff and class members have been injured and are entitled to damages in an amount to be proven at trial.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Class)

101. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

102. Pursuant to the FTC Act, 15 U.S.C. § 45, Dickey's had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and class members' personal information.

103. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Dickey's, of failing to use reasonable measures to protect Card Information.

The FTC publications and orders described above also form part of the basis of Dickey's duty to protect Plaintiffs' and class members' sensitive information.

104. Dickey's violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Card Information and not complying with applicable industry standards, including PCI DSS, as described in detail herein. Dickey's conduct was particularly unreasonable given the nature and amount of Card Information it collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to consumers and financial institutions.

105. The harm that has occurred is the type of harm the FTC Act (and similar state statutes) is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the class.

106. Dickey's had a duty to Plaintiff and class members to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and class members' personal information.

107. Dickey's breached its duties to Plaintiff and class members under the FTC Act (and similar state statutes), by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and class members' financial and personal information.

108. Dickey's' violation of Section 5 of the FTC Act (and similar state statutes) and its failure to comply with applicable laws and regulations constitutes negligence per se.

109. But for Dickey's wrongful and negligent breach of its duties owed to Plaintiff and class members, they would not have been injured.

110. The injury and harm suffered by Plaintiff and class members was the reasonably foreseeable result of Dickey's' breach of its duties. Dickey's knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiff and class members to suffer the foreseeable harms associated with the exposure of their Card Information.

111. Had Plaintiff and class members known that Dickey's did and does not adequately protect customer Card Information, they would not have made purchases at Dickey's locations.

112. As a direct and proximate result of Dickey's negligence per se, Plaintiff and class members have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made at Dickey's that Plaintiff and class members would not have made had they known of Dickey's careless approach to cyber security; lost control over the value of personal information; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Card Information, entitling them to damages in an amount to be proven at trial.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

113. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

114. Plaintiff and class members who made purchases at Dickey's locations during the period in which the Data Breach occurred had implied contracts with Dickey's.

115. Specifically, Plaintiff and class members paid money to Dickey's and, in connection with those transactions, provided Dickey's with their Card Information. In exchange, Dickey's agreed, among other things: (1) to provide food, gasoline, and food services to Plaintiff and class members at its various locations; (2) to take reasonable measures to protect the security and confidentiality of Plaintiff's and class members' Card Information; and (3) to protect Plaintiff's and class members' personal information in compliance with federal and state laws and regulations and industry standards.

116. Protection of personal information is a material term of the implied contracts between Plaintiff and class members, on the one hand, and Dickey's, on the other hand. Indeed, as set forth, *supra*, Dickey's recognized the importance of data security and privacy of customers' sensitive financial information in the privacy policy. Had Plaintiff and class members known that Dickey's would not adequately protect customer Card Information, they would not have made purchases at Dickey's locations.

117. Dickey's did not satisfy its promises and obligations to Plaintiff and class members under the implied contracts because it did not take reasonable measures to keep their personal information secure and confidential and did not comply with the applicable laws, regulations, and industry standards.

118. Dickey's materially breached its implied contracts with Plaintiff and class members by failing to implement adequate payment card and Card Information security measures.

119. Plaintiff and class members fully performed their obligations under their implied contracts with Dickey's.

120. Dickey's' failure to satisfy its obligations led directly to the successful intrusion of Dickey's computer servers and stored Card Information and led directly to unauthorized parties' access and exfiltration of Plaintiff's and class members' Card Information.

121. Dickey's breached these implied contracts as a result of its failure to implement security measures.

122. Also, as a result of Dickey's failure to implement the security measures, Plaintiff and class members have suffered actual damages resulting from the theft of their personal information and remain at imminent risk of suffering additional damages in the future.

123. Accordingly, Plaintiff and class members have been injured as a proximate result of Dickey's breaches of implied contracts and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

124. Plaintiff realleges and incorporates paragraphs 1–89 as though fully set forth herein.

125. This claim is plead in the alternative to the above implied contract claim.

126. Plaintiff and class members conferred a monetary benefit upon Dickey's in the form of monies paid for the purchase of food at its locations.

127. Dickey's appreciated or had knowledge of the benefits conferred upon them by Plaintiff and class members. Dickey's also benefited from the receipt of Plaintiff's and class members' Card Information, as this was utilized by Dickey's to facilitate payment to it.

128. The monies for food, dining, and food-related services that Plaintiff and class members paid to Dickey's were supposed to be used by Dickey's, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

129. As a result of Dickey's conduct, Plaintiff and class members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiff and class members paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

130. Under principals of equity and good conscience, Dickey's should not be permitted to retain the money belonging to Plaintiff and class members because Dickey's failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

131. Dickey's should be compelled to disgorge into a common fund for the benefit of Plaintiff and class members all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

VI. PRAYER FOR RELIEF

Plaintiff, on behalf of herself and the class, respectfully requests that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23(a) and (b), and, pursuant to Fed. R. Civ. P. 23(g), appoint Plaintiff as class representative and her counsel as class counsel.

B. Award Plaintiff and the class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement.

C. Award Plaintiff and the class equitable, injunctive, and declaratory relief as may be appropriate. Plaintiff, on behalf of the class, seeks appropriate injunctive relief designed to ensure against the recurrence of a data breach by adopting and implementing best security data practices to safeguard customers' financial and personal information, extend credit monitoring services and similar services to protect against all types of identity theft, especially including card theft and fraudulent card charges, and to provide elevated credit monitoring services to minor and elderly class members who are more susceptible to fraud and identity theft.

D. Award Plaintiff and the class pre-judgment and post-judgment interest to the maximum extent allowable.

E. Award Plaintiff and the class reasonable attorneys' fees and costs as allowable.

F. Award Plaintiff and the class such other favorable relief as allowable under law or at equity.

Dated: November 16, 2020

Respectfully submitted,

By: /s/ Cory S. Fein

Cory S. Fein (Texas Bar No. 06879450)
CORY FEIN LAW FIRM
712 Main Street, Suite 800
Houston, TX 77002
(281) 254-7717
(530) 748 - 0601 (fax)
cory@coryfeinlaw.com

Benjamin F. Johns (*pro hac vice* to be filed)
Samantha E. Holbrook (*pro hac vice* to be filed)
Andrew W. Ferich (*pro hac vice* to be filed)
Alex M. Kashurba (*pro hac vice* to be filed)
CHIMICLES SCHWARTZ KRINER & DONALDSON-SMITH LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041
(610) 642-8500
bfj@chimicles.com
awf@chimicles.com
seh@chimicles.com
amk@chimicles.com

Ben Barnow (*pro hac vice* to be filed)
Erich P. Schork (*pro hac vice* to be filed)
Anthony L. Parkhill (*pro hac vice* to be filed)
BARNOW AND ASSOCIATES, P.C.
205 W. Randolph St., Suite 1630
Chicago, IL 60606
Tel: (312) 621-2000
Fax: (312) 641-5504
b.barnow@barnowlaw.com
e.schork@barnowlaw.com
aparkhill@barnowlaw.com

Counsel for Plaintiff