UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

LLOYD F. COLLINS, individually and on behalf of all others similarly situated, Plaintiff, vs. RUTTER'S INC. Defendant.	Case No. _____ Civil Action **Jury Trial Demanded** **COMPLAINT - CLASS ACTION**

Plaintiff Lloyd F. Collins ("Plaintiff"), on behalf of himself and all others similarly situated, brings this class action complaint against Defendant Rutter's, Inc. (*f/k/a*, Rutter's Farm Stores Inc.; *d/b/a*, Rutter's) ("Rutter's" or "Defendant"). Plaintiff alleges the following upon personal knowledge as to his own acts and experiences, and upon the investigation of his attorneys and review of public documents as to all other matters.

I. INTRODUCTION

1. This is a data breach class action on behalf of consumers whose credit and debit card information ("Payment Card" or "Payment Cards") was accessed by unauthorized users as part of a large cyber-attack of Rutter's Payment Card environment and systems.

2. Rutter's reported that between at least August 30, 2018 and May 29,

2019 (the "Breach Period"), hackers gained access to its stores' network system and planted malware on its point-of-sale ("POS") devices in its stores and at its gas pumps, which collected customers' Payment Card information (the "Data Breach"). Information compromised in the breach included Payment Card numbers, card expiration dates, security codes (commonly referred to as "CVV" numbers), and customers' names ("Card Information").

3. At least one cybersecurity expert has instructed consumers who believe they have been impacted by the Rutter's Data Breach to cancel their Payment Cards immediately: "If you do believe that you are a victim, that you have used a credit card at a Rutter's store, I would cancel that credit card immediately," said John Sancenito, the president of Information Network Associates, which helps companies with recovery after data breaches.[1] Mr. Sancenito advised further: "If you happened to use your debit card, go to your bank and get a new debit card, and you might want to also start thinking about changing any pin numbers or passwords."[2] Notably, this advice is at odds with Rutter's statement that affected customers should simply "review your payment card statements for any unauthorized activities." The stolen Card Information is a valuable commodity to identity thieves. William P. Barr, the United States Attorney General, made clear that consumers' sensitive personal

[1] *See* https://www.abc27.com/news/local/york/legislator-security-expert-weigh-in-on-rutters-data-breach/ (last visited March 4, 2020).
[2] *Id*.

information commonly stolen in data breaches "has economic value."[3]

4. As a result of the Data Breach, many Rutter's customers—including Plaintiff—have experienced and will continue to experience fraudulent purchases and other misuse related to their accounts. These Class Members will also incur out-of-pocket costs to purchase protective measures such as credit monitoring services, credit freezes, and credit reports. They will also incur costs associated with obtaining replacement cards and other items directly and indirectly related to the Data Breach.

5. Plaintiff has sustained actual, palpable fraud and injury as a result of the Data Breach. Plaintiff and Class Members have also been exposed to a heightened and imminent risk of fraud and identity theft. Because of the Data Breach, they must now and in the future closely monitor their financial accounts to guard against fraud. This is a burdensome and time-consuming process.

6. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Card Information was stolen in the Data Breach. Plaintiff seeks remedies including reimbursement of fraud losses and other out-of-pocket costs, compensation for time spent in response to the Data Breach, credit monitoring and identity theft insurance, and injunctive relief requiring substantial improvements to Rutter's card payment data security systems.

---

[3] *See* https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military (last visited March 4, 2020).

II. PARTIES

A. Plaintiff

7. Plaintiff Lloyd F. Collins is an adult residing in Shippensburg, Pennsylvania. On September 2, 15, and 20, October 1 and 5, and December 12, 2018, Mr. Collins used his Chase credit card to make purchases at Rutter's Shippensburg store (Store #31), during the Breach Period. Rutter's website lists its Shippensburg store (Store #31) as one of its locations that was breached between at least October 1, 2018 and May 29, 2019.[4]

8. On February 24, 2020, Mr. Collins discovered that his Chase credit card had been used to make a fraudulent purchase that same day in the amount of $2,477 at United Airlines. Mr. Collins received a text message on his cell phone from Chase Fraud Recovery Department on February 24, 2020, notifying him of this fraudulent charge, and Mr. Collins contacted Chase that same day to dispute the charge. Chase cancelled his credit card and sent him a replacement card, but it took several days before he received it in the mail, during which time he was without the benefit of using his credit card to make everyday transactions.

9. Although Chase reimbursed Mr. Collins for the fraudulent charge, it did not do so for (upon information and belief) approximately three business days.

[4] *See* https://www.rutters.com/notice-of-payment-card-incident-locations/ (last visited March 4, 2020).

During that time, Mr. Collins was without the funds used to make this fraudulent charge. Mr. Collins has suffered immense frustration, aggravation and loss of time calling Chase, discussing this situation with Chase, disputing the fraudulent charge, and changing his card information with every vendor whose bills Mr. Collins pays using his Chase account on a recurring basis. Mr. Collins estimates that he has already spent approximately five hours engaging in the foregoing remedial actions, and he continues to spend additional time dealing with the Data Breach. Furthermore, Mr. Collins contacted one of the major credit bureaus to set up fraud alerts for his credit history, to prevent future identity theft. Mr. Collins suffered additional harm in the form of aggravation and lost time by checking his credit and contacting this credit bureau to set up this fraud alert. Prior to this fraudulent charge, Mr. Collins had never previously suffered fraudulent activity on his Chase account.

B. Defendant

10. Defendant Rutter's, Inc. is a privately held company with its principal place of business in York, Pennsylvania. It is incorporated in Pennsylvania, and its headquarters is located at 2100 North George Street, York, Pennsylvania 17404. It operates 72 convenience stores in Central Pennsylvania, West Virginia, and Maryland, many of which also have gas pumps.

III. JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction under the Class Action

Fairness Act, 28 U.S.C. § 1332(d) because this is a class action involving more than 100 Class Members, the amount in controversy exceeds $5 million, and many members of the class are citizens of states different from Rutter's.

12. This Court has personal jurisdiction over Rutter's because Rutter's is (1) incorporated and headquartered in Pennsylvania, (2) conducts substantial business in and throughout Pennsylvania, and (3) the wrongful acts alleged in the Complaint were committed largely in Pennsylvania.

13. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because Rutter's is headquartered in this District, and as a result a substantial part of the events giving rise to Plaintiff's claims occurred in this District. Venue is also proper because Rutter's regularly transacts business here.

IV. FACTUAL ALLEGATIONS

A. The Rutter's Data Breach

14. Rutter's is an operator of a large chain of convenience stores and gas stations.

15. On February 13, 2020, Rutter's publicly announced the Data Breach by stating the following on its website[5]:

[5] https://www.rutters.com/paymentcardincident/ (last visited March 4, 2020).

> Rutter's recently received a report from a third party suggesting there may have been unauthorized access to data from payment cards that were used at some Rutter's locations. We launched an investigation, and cybersecurity firms were engaged to assist. We also notified law enforcement.
>
> On January 14, 2020, the investigation identified evidence indicating that an unauthorized actor may have accessed payment card data from cards used on point-of-sale (POS) devices at some fuel pumps and inside some of our convenience stores through malware installed on the payment processing systems. The malware searched for track data (which sometimes has the cardholder name in addition to card number, expiration date, and internal verification code) read from a payment card as it was being routed through the payment processing systems …. As a result, for EMV cards inserted into the chip-reader on the EMV POS devices in our convenience stores, only card number and expiration date (and not the cardholder name or internal verification code) were involved ….
>
> The specific timeframes when data from cards used at the locations involved may have been accessed vary by location over the general timeframe beginning October 1, 2018 through May 29, 2019. There is one location where access to card data may have started August 30, 2018 and nine additional locations where access to card data may have started as early as September 20, 2018 …. For those customers Rutter's can identify as having used their card at a location involved during that location's specific timeframe and for whom Rutter's has a mailing address or email address, Rutter's will be mailing them a letter or sending them an email ….

16. Thus, Rutter's did not discover the Data Breach for nearly *eighteen months* and did not notify consumers of the Data Breach for more than a month after discovering it.

17. As reported by Rutter's and numerous news outlets, "the information generally believed to have been collected is customers' names, card numbers,

expiration dates, and internal verification codes. But for users who paid with cards at POS devices that accept EMV-capable cards, the malware collected only the card numbers and expiration dates."[6]

18. Rather than proactively taking steps to help consumers deal with and avoid damage from the Data Breach, Rutter's placed the burden on consumers to protect themselves:

> It is always advisable to review your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to your card issuer because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of your payment card. Please see the section below for information on additional steps you may take.[7]

19. Similarly, Rutter's opted not to provide credit monitoring services free of charge to impacted consumer—as many breached companies have done in the past—and instead merely instructed consumers to monitor their credit themselves:

> **Additional Steps You Can Take**
>
> It is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your free annual credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

---

[6] *See* https://www.insurancebusinessmag.com/us/news/cyber/rutters-store-chain-reveals-malware-attacked-its-pos-system-214097.aspx (last visited March 4, 2020).
[7] https://www.rutters.com/paymentcardincident/ (last visited March 4, 2020).

- Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.[8]

20. Thus, rather than providing meaningful assistance to consumers to help deal with the fraud that has and will continue to result from the Data Breach, Rutter's simply told them to carefully monitor their own accounts and remain "vigilant" for fraud. In contrast to what is and has been frequently made available to consumers in recent data breaches, Rutter's has not offered or provided any monitoring service or fraud insurance to date.

21. Even though Rutter's disclosed that some of the Card Information accessed through the Data Breach did not include CVV numbers (the three or four-digit security code printed on the back of credit and debit cards), thieves reportedly can still make fraudulent purchases without access to the security code:

[T]hree- or four-digit security codes weren't stolen, but that doesn't

[8] https://www.rutters.com/paymentcardincident/ (last visited March 4, 2020).

> necessarily matter for the hackers, per [cybersecurity expert Matthew] Wilson. A three-digit code has only 999 possible answers, after all. "That sounds like lot to human," he says. "To a machine, it's nothing."[9]

22. Rutter's failed to properly safeguard Class Members' Card Information, allowing malware to be present on—and cybercriminals to access Payment Card Information from—its systems for as many as *nine months* completely undetected. Rutter's also failed to properly monitor its systems. Had it properly done so, Rutter's would have discovered the malware much sooner than *eighteen months* after the breach began. Indeed, Rutter's reported that it "received a report from a third party" of the Data Breach. Had the unnamed third-party not notified Rutter's of the Data Breach, it presumably would have gone undetected even longer than it did.

23. Rutter's had a continuing duty pursuant to common law, industry standards, card network rules, and representations made in its own privacy policy to keep consumers' Card Information confidential and to protect it from unauthorized access.

B. Rutter's Was on Notice of a Significant Risk of a Data Breach

24. Rutter's data security obligations were particularly important and well-known to it given the substantial increase in payment card data breaches throughout

[9] https://www.phillymag.com/news/2019/12/20/wawa-data-breach/ (last visited March 4, 2020).

the retail industry preceding the Data Breach, including numerous recent malware-based payment card breaches. The increase in data breaches, and the risk of future breaches, was widely known throughout the retail industry, including to Rutter's.

25. Indeed, during the Breach Period, Visa warned gas station operators, such as Rutter's, about an increase in hackers targeting internal payment processing systems at gas stations. The warning specified that hackers have been targeting internal processing systems, not just external card-swipe terminals attached to gas pumps. Specifically, Visa distributed a "Security Alert" dated November 2019, stating the following:

> In August and September 2019, Visa Payment Fraud Disruption (PFD) investigated two separate breaches at North American fuel dispenser merchants. The attacks involved the use of point-of-sale (POS) malware to harvest payment card data from fuel dispenser merchant POS systems. It is important to note that **this attack vector differs significantly from skimming at fuel pumps, as the targeting of POS systems requires the threat actors to access the merchant's internal network** ….
>
> **The targeting of fuel dispenser merchants is the result of the slower migration to chip technology on many terminals, which makes these merchants an attractive target for criminal threat actors attempting to compromise POS systems for magnetic stripe payment card data** ….
>
> The [hackers] gain access to the targeted merchant's network, move laterally within the network using malware toolsets, and ultimately target the merchant's POS environment to scrape payment card data. The groups also have close ties with the cybercrime underground and are able to easily monetize the accounts obtained in these attacks by selling the accounts to the top tier cybercrime underground carding shops.

> Fuel dispenser merchants should take note of this activity as the group's operations are significantly more advanced than fuel dispenser skimming, and these attacks have the potential to compromise a high volume of payment accounts. The deployment of devices that support chip will significantly lower the likelihood of these attacks.[10]

26. The Visa warning specified that hackers were placing "malware" onto card processing systems. Notably, Rutter's reported that malware was placed on its gas pumps.[11]

27. The Visa warning also specified that hackers were attacking gas station merchants that had not yet upgraded to chip technology. Although Rutter's reported that it utilizes chip readers at POS terminals inside *some* of its stores, its notice is silent as to its implementation, and use of, chip readers at its gas pumps. The Visa warning placed Rutter's on further notice of an unusually high risk of a data breach. Rutter's failed to improve its cardholder data security despite these known critical risks.

C. Previous Credit Card Data Breach at Rutter's

28. Rutter's has a history of credit card intrusions. In 2017, police investigated multiple skimming devices placed on various Rutter's ATMs.[12]

---

[10] Visa Security Alert (November 2019), *available at* https://usa.visa.com/dam/VCOM/global/support-legal/documents/visa-security-alert-attacks-targeting-fuel-dispenser-merchant-pos.pdf (last visited March 4, 2020) (emphasis added).

[11] https://www.rutters.com/paymentcardincident/ (last visited March 4, 2020).

[12] *See* https://www.yorkdispatch.com/story/news/2017/03/08/eight-accused-card-skimming-york-county/98909806/ (last visited February 25, 2020); *see also*

29. These breaches, coupled with numerous others affecting other retail companies, put Rutter's on notice of the importance of data security, the fact that thieves were aggressively seeking stolen credit card information from Rutter's, and the harm that could result from weak data security. Despite these events, Rutter's nevertheless failed to adopt adequate data security governing its credit and debit card transactions.

D. Rutter's Privacy Policy

30. Rutter's Privacy Policy stated that data security is important to the Company, and that it is committed to safeguarding consumer data:

> HOW we protect and RETAIN your information
> **We and our Service Providers take security measures to protect against unauthorized access to or unauthorized alteration, disclosure, or destruction of data**. These include firewalls and encryption, internal reviews of our Service Providers data collection, storage and processing practices, and security measures, **as well as physical security measures to guard against unauthorized access to systems**.[13]

31. Plaintiff and Class Members provided their Card Information to Rutter's with the reasonable expectation that Rutter's would comply with its obligations to keep the card information confidential and would secure it from unauthorized access. Rutter's failed to do so, in contravention of its own privacy

---

https://www.ydr.com/story/news/2017/03/07/atm-rutters-shrewsbury-card-skimming-check-bank-account/98873454/ (last visited February 25, 2020).

[13] *See* https://www.rutters.com/privacy-policy/ (emphasis added) (last visited March 4, 2020).

policy.

E. Rutter's Data Security Failures

32. Rutter's breached its duties, obligations, and promises by, *inter alia*, failing to:

(a) adequately safeguard consumers' Card Information;

(b) maintain an adequate data security environment to reduce the risk of a data breach;

(c) properly monitor its data security systems for existing intrusions and weaknesses;

(d) perform penetration tests to determine the strength of its payment card processing systems;

(e) properly train its information technology staff on matters relevant to cardholder data security; and

(f) retain outside vendors to periodically test its payment card processing systems.

1. *Rutter's Violated PCI Data Security Standards*

33. There is an extensive network of financial institutions, card-issuing banks, and card-processing companies involved in credit and debit card transactions. Card networks have issued detailed rules and standards governing the basic protective measures that merchants like Rutter's must take to ensure that payment card information is properly safeguarded.

34. The payment card networks (primarily MasterCard, Visa, American Express, and Discover) have issued card operating rules that are binding on merchants including Rutter's and require merchants to protect cardholder data. In

particular, the Payment Card Industry Security Standards Council promulgates minimum standards that apply to all organizations that store, process, or transmit payment card data. These standards are known as the Payment Card Industry Data Security Standards ("PCI DSS"). PCI DSS is the industry standard governing the security of credit and debit card data.

35. PCI DSS establishes detailed comprehensive requirements for satisfying each of the following twelve "high-level" mandates:[14]

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

36. As noted in the chart, PCI DSS required Rutter's to "protect all systems against malware." Rutter's failed to do so. Rutter's specified that the hacker(s) placed "malware" on Rutter's payment processing servers.

[14] *Payment Card Industry (PCI) Data Security Standard*, PCI Security Standards Council, May 2018, at p. 5, *available at* https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1577046042482 (last visited Jan. 9, 2020).

37. PCI DSS also required Rutter's to "[t]rack and monitor all access to network resources." Rutter's failed to do so. The hacker(s) had access to Rutter's system for as long as nine months, illustrating that Rutter's had materially deficient tracking and monitoring systems in place.

38. Upon information and belief, Rutter's violated numerous other provisions of the PCI DSS, including subsections underlying the chart above. Those deficiencies will be revealed during discovery with the assistance of expert witnesses.

39. PCI DSS sets the minimum level of what must be done, not the maximum. While PCI compliance is an important first step in securing cardholder data, it is not sufficient on its own to protect against all breaches, nor does it provide a safe harbor against civil liability for a data breach.

40. At all relevant times, Rutter's was well-aware of its PCI DSS obligations to protect cardholder data. Rutter's was an active participant in the payment card networks as it collected and likely transmitted thousands (or more) of sets of payment card data per day.

41. Industry experts acknowledge that a data breach is indicative of data security failures. For example, research and advisory firm Aite Group has stated: "'If your data was stolen through a data breach that means you were somewhere out

of compliance' with payment industry data security standards."[15]

2. *Rutter's Violated the FTC Act*

42. The Federal Trade Commission ("FTC") has held that the failure to employ reasonable 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 ("FTCA"), 15 U.S.C. §45.

43. The FTC published guidance establishing reasonable data security practices for businesses. The FTC guidance notes that businesses should (among other things): protect the personal customer information that they acquire; 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 vulnerabilities. FTC guidance also recommends that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating that someone may be trying to penetrate the system; and watch for large amounts of data being transmitted from the system.[16]

---

[15] Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May 26, 2017) (accessible at: https://www.reuters.com/article/us-chipotle-cyber/chipotle-says-hackers-hit-most-restaurants-in-data-breach-idUSKBN18M2BY) (last visited March 4, 2020).
26, 2017), *available at* http://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY (last accessed Jan. 9, 2020).

[16] *See, e.g.*, *Start with Security: A Guide for Business*, Federal Trade Commission,

44. The FTC has issued orders against businesses for failing to employ reasonable measures to safeguard customer data. The orders provide further public guidance to businesses concerning their data security obligations.

45. Rutter's knew or should have known about its obligation to comply with the FTC Act regarding data security.

46. Rutter's misconduct violated the FTC Act, led to the Data Breach, and caused harm to Plaintiff and Class Members.

F. Misuse of the Stolen Data Has Begun

47. Widespread misuse of the stolen cardholder data has already begun.

48. Plaintiff has suffered at least one fraudulent charge on his payment card, as discussed in detail above.

49. Indeed, at least one cybersecurity expert has instructed consumers who believe they have been impacted by the Rutter's Data Breach to cancel their Payment Cards immediately: "If you do believe that you are a victim, that you have used a credit card at a Rutter's store, I would cancel that credit card immediately," said John Sancenito, the president of Information Network Associates, which helps companies

---

June 2015, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; *Protecting Personal Information: A Guide for Business*, Federal Trade Commission, Oct. 2016, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

with recovery after data breaches.[17] Mr. Sancenito advised further: "If you happened to use your debit card, go to your bank and get a new debit card, and you might want to also start thinking about changing any pin numbers or passwords."[18] Notably, this advice is at odds with Rutter's statement that affected customers should simply "review your payment card statements for any unauthorized activities."

G. Damages to Class Members

50. The Data Breach is particularly alarming given that it reportedly lasted as long as nine months. Each Plaintiff and the Class Members have been damaged by the compromise of their Card Information in the Data Breach.

51. Class Members also face a substantial and imminent risk of fraudulent charges on their Payment Cards. Criminals carried out the Data Breach and stole the Card Information with the intent to use it for fraudulent purposes and/or to sell it.

52. Plaintiff and Class Members have already experienced fraudulent credit and debit card purchases, and other Class Members will experience fraud going forward.

53. Also, many Class Members will incur out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, fees for replacement cards, and similar costs related to the Data Breach.

---

[17] *See* https://www.abc27.com/news/local/york/legislator-security-expert-weigh-in-on-rutters-data-breach/ (last visited March 4, 2020).
[18] *Id.*

54. Class Members also suffered a "loss of value" of their credit and debit card information when it was stolen by the hacker in the Data Breach. A robust market exists for stolen card information, which is sold on the dark web at specific identifiable prices. This market serves as a means to determine the loss of value to Class Members.

55. Class Members also suffered "benefit of the bargain" damages. Class Members overpaid for goods that should have been – but were not – accompanied by adequate data security. Part of the price Class Members paid to Rutter's was intended to be used to fund adequate data security. Class Members did not get what they paid for.

56. Class Members have spent and will continue to spend substantial amounts of time monitoring their payment card accounts for fraud, disputing fraudulent transactions, and reviewing their financial affairs more closely than they otherwise would have done but for the Data Breach. Class Members will also spend time obtaining replacement cards and resetting automatic payment links to their new cards. These efforts are burdensome and time-consuming.

57. Class Members who experience actual fraud will also be harmed by the inability to use their credit or debit cards when their accounts are suspended or otherwise rendered unusable due to the fraudulent charges. To the extent Class Members are charged monthly/annual fees for their Payment Cards and/or attendant

accounts, they are left without the benefit of that bargain while they await receipt of their replacement cards. Class Members will also be harmed by the loss of use of and access to their account funds and credit lines, or being limited in the amount of money they are permitted to obtain from their accounts. Class Members will further be harmed by the loss of rewards points or airline mileage available on credit cards that consumers lost credit for as a result of having to use alternative forms of payment while awaiting replacement cards. This includes missed payments on bills and loans, late charges and fees, and adverse effects on their credit, including decreased credit scores and adverse credit notations.

58. The stolen Card Information is a valuable commodity to identity thieves. William P. Barr, the United States Attorney General, made clear that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[19] The purpose of stealing large caches of Card Information is to use it to defraud consumers or to place it for illegal sale and to profit from other criminals who buy the data and use it to commit payment card fraud. Indeed, cyber criminals routinely post stolen payment card information on anonymous websites, making the information widely available to a criminal underworld. There is an active and robust market for this information. One commentator discussing the Rutter's

[19] *See* https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military (last visited March 4, 2020).

breach noted that "Most of the time what [data breach hackers] do is they steal the data and then they sell the data on the dark web to the people who actually commit the fraud."[20] Thus, upon information and belief, Class Members' Card Information was stolen and was likely illegally placed for sale on the "dark web"—an underground or "black market" 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, and counterfeit money).

59. The risk of fraud will persist for years. Identity thieves often hold stolen data for months or years before using it, to avoid detection. Also, the sale of stolen information on the dark web may take months or more to reach end-users, in part because the data is often sold in small batches as opposed to in bulk to a single buyer.

60. Thus, Class Members must vigilantly monitor their financial accounts for months or years to come.

H. Class Members Face a Risk of Identity Theft Beyond Just Credit and Debit Card Fraud

61. Identity thieves can combine data stolen in the Data Breach with other information about Class Members gathered from underground sources, public sources, or even Class Members' social media accounts. Thieves can use the

[20] *See* https://www.abc27.com/news/local/york/legislator-security-expert-weigh-in-on-rutters-data-breach/ (last visited March 4, 2020).

combined data to send highly targeted phishing emails to Class Members to obtain more sensitive information. Thieves can use the combined data to commit potential crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

62. Rutter's has acknowledged that Class Members face a significant risk of various types of identity theft stemming from the Data Breach. Shifting the burden of responding to the Data Breach to consumers, Rutter's recommended that affected customers undertake the following daunting tasks: (i) "review[] your account statements and free credit reports for any unauthorized activity"; (ii) "obtain a copy of your credit report"; (iii) "[i]f you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state"; (iv) "contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records."; (v) "place 'fraud alerts' in your file to let potential creditors and others know that you may be a victim of identity theft"; (vi) "separately place a security freeze on your credit file at each credit reporting

company"; (vii) "contact each of the [three separate] credit reporting agencies [Experian Security Freeze, Transunion Security Freeze, and Equifax Security Freeze]."[21]

63. Thus, Rutter's acknowledges that Class Members face a risk of identity theft beyond just fraudulent credit and debit card transactions.

64. Rutter's has taken no affirmative steps—beyond notifying consumers of the Data Breach—to protect against these broad-based types of fraud, such as offering free credit monitoring and identity theft insurance to all customers whose card information was stolen in the Data Breach. Rutter's efforts are wholly insufficient to combat the indefinite undeniable risk of fraud and identity theft.

V. CLASS ACTION ALLEGATIONS

65. Plaintiff brings this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of a Nationwide Class. In the alternative, Plaintiff brings this case on behalf of a Pennsylvania Class (collectively, the "Classes"), defined as follows:

> Nationwide Class: All persons in the United States whose credit or debit card numbers were compromised in the data breach announced by Rutter's on February 13, 2020.
>
> Pennsylvania Class: All residents of the Commonwealth of Pennsylvania whose credit or debit card numbers were compromised in the data breach announced by Rutter's on February 13, 2020.

[21] *See* https://www.rutters.com/paymentcardincident/ (last visited March 4, 2020).

66. Excluded from the Classes are Rutter's executive officers, and the judge to whom this case is assigned.

67. Numerosity. The Classes are each so numerous that joinder of all members is impracticable. On information and belief, the Nationwide Class consists of hundreds to thousands or more individuals, and the Pennsylvania Class consists of hundreds to thousands or more individuals. These estimates are based on the fact that the Data Breach affected most (if not all) of Rutter's 72 convenience store locations, as well as its gas pumps, for a nine-month period.

68. Commonality. There are many questions of law and/or fact common to Plaintiff and the Classes. Common questions include, but are not limited to, the following:

(a) Whether Rutter's data security systems prior to and during the Data Breach complied with applicable data security laws, regulations, industry standards, and PCI DSS requirements;

(b) Whether Rutter's owed a duty to Class Members to safeguard their Card Information;

(c) Whether Rutter's breached its duty to Class Members to safeguard their Card Information;

(d) Whether a computer hacker obtained Class Members' Card Information in the Data Breach;

(e) Whether Rutter's knew or should have known that its data security systems and monitoring processes were deficient;

(f) Whether Plaintiff and Class Members suffered legally cognizable damages as a result of the Data Breach; and

(g) Whether Plaintiff and Class Members are entitled to injunctive relief.

69. Typicality. Plaintiff's claims are typical of the claims of all Class Members because Plaintiff, like other Class Members, suffered a theft of his Card Information in the Data Breach.

70. Adequacy of Representation. Plaintiff will fairly and adequately protect the interests of the Classes. Plaintiff has retained competent and capable counsel with significant experience in complex class action litigation, including data breach class actions. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the Classes. Plaintiff's counsel has the financial and personnel resources to do so. Neither Plaintiff nor his counsel have interests that are contrary to, or that conflict with, those of the Classes.

71. Predominance. Rutter's has engaged in a common course of conduct toward all Class Members. The common issues arising from Rutter's conduct predominate over any issues affecting just individual Class Members. Adjudication of the common issues in a single action has important and desirable advantages of judicial economy.

72. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would find that the cost of

litigating their individual claim is prohibitively high, and they would have no effective remedy on an individual non-class basis. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to Class Members, which would establish incompatible standards of conduct for Rutter's. In contrast, conducting this action on a class-wide basis presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of all Class Members.

73. Rutter's has acted on grounds that apply generally to the Classes as a whole, so that injunctive relief is appropriate on a class-wide basis pursuant to Fed. R. Civ. P. 23(b)(2).

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff, the Nationwide Class, and, in the alternative, the Pennsylvania Class)

74. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

75. Rutter's obtained Class Members' Payment Card Information in connection with Class Members' purchases at Rutter's stores and gas pumps.

76. By collecting and maintaining cardholder data, Rutter's had a duty of care to use reasonable means to secure and safeguard the Card Information and to prevent disclosure of the information to unauthorized individuals. Rutter's duty

included a responsibility to implement processes by which it could detect a data breach of this type and magnitude in a timely manner.

77. Rutter's owed a duty of care to Plaintiff and Class Members to provide data security consistent with the various requirements and rules discussed above.

78. Rutter's duty of care arose as a result of, among other things, the special relationship that existed between Rutter's and its customers. Rutter's was in position to ensure that its systems were sufficient to protect against the foreseeable risk that a data breach could occur, which would result in substantial harm to consumers.

79. Also, Rutter's had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, failing to use reasonable measures to protect confidential consumer data.

80. Rutter's duty to use reasonable care in protecting cardholder data arose not only as a result of the statutes and regulations described above, but also because Rutter's is bound by industry standards and PCI DSS rules to protect Card Information.

81. Rutter's was subject to an "independent duty" untethered to any contract between Class Members and Rutter's.

82. Rutter's breached its duties, and thus was negligent, by failing to use reasonable measures to protect cardholder information. Rutter's negligent acts and omissions include, but are not limited to, the following:

(a) Failing to adopt, implement, and maintain adequate security measures to safeguard Card Information;

(b) Failing to adequately monitor the security of Rutter's Payment Card processing network;

(c) Allowing unauthorized access to Class Members' sensitive Card Information;

(d) Failing to detect in a timely manner that Class Members' Card Information had been compromised; and

(e) Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the risk of identity theft and other damages.

83. It was foreseeable to Rutter's that a failure to use reasonable measures to protect Card Information could result in injury to consumers. Further, actual and attempted breaches of data security were reasonably foreseeable to Rutter's given the known frequency of Payment Card data breaches: (i) in the retail industry in general, (ii) at gas stations in particular, and (iii) at Rutter's operations specifically.

84. Plaintiff and Class Members suffered various types of damages as alleged above.

85. Rutter's wrongful conduct was a proximate cause of Class Members' damages.

86. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

87. Plaintiff and Class Members are also entitled to injunctive relief requiring Rutter's to (among other things): (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide several years of free credit monitoring and identity theft insurance to all Class Members.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff, the Nationwide Class, and, in the alternative, the Pennsylvania Class)

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

89. As alleged above, pursuant to the FTC Act, 15 U.S.C. § 45, Rutter's had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Card Information.

90. 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 Rutter'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 Rutter's duty.

91. Rutter'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. Rutter'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.

92. 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.

93. Rutter'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' Card Information.

94. Rutter'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' Card Information.

95. Rutter'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*.

96. But for Rutter's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

97. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Rutter's breach of its duties. Rutter'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.

98. Had Plaintiff and Class Members known that Rutter's did and does not adequately protect customer Card Information, they would not have made purchases at Rutter's stores and gas pumps.

99. As a direct and proximate result of Rutter's negligence *per se*, Plaintiff and Class Members have suffered harm, including but not limited to 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 Rutter's that Plaintiff and Class Members would not have made had they known of Rutter's careless approach to cyber security; lost control over the value of Card 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, the Nationwide Class, and, in the alternative, the Pennsylvania Class)

100. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

101. When Plaintiff and Class Members provided their Card Information to Rutter's in exchange for Rutter's products, they entered into implied contracts with Rutter's under which Rutter's agreed to take reasonable steps to protect the Card Information.

102. Rutter's solicited and invited Class Members to provide their Card Information as part of Rutter's regular business practices. Plaintiff and Class Members accepted Rutter's offers and provided their Card Information to Rutter's.

103. When entering into the implied contracts, Plaintiff and Class Members reasonably believed and expected that Rutter's data security practices complied with relevant laws, regulations, and industry standards.

104. Rutter's implied promise to safeguard Card Information is evidenced by, e.g., the representations in Rutter's Privacy Policy set forth above.

105. Plaintiff and Class Members paid money to Rutter's to purchase items at Rutter's convenience stores and gas at Rutter's gas pumps. Plaintiff and Class Members reasonably believed and expected that Rutter's would use part of those funds to obtain adequate data security. Rutter's failed to do so.

106. Plaintiff and Class Members would not have provided their Card Information to Rutter's in the absence of Rutter's implied promise to keep the Card Information reasonably secure.

107. Plaintiff and Class Members fully performed their obligations under the implied contracts by paying money to Rutter's.

108. Rutter's breached its implied contracts with Plaintiff and Class Members by failing to implement reasonable data security measures.

109. As a direct and proximate result of Rutter's breaches of the implied contracts, Plaintiff and Class Members sustained damages as alleged herein.

110. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

111. Plaintiff and Class Members are also entitled to injunctive relief requiring Rutter's to (among other things): (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and

(iii) provide several years of free credit monitoring and identity theft insurance to all Class Members.

COUNT IV
VIOLATIONS OF THE PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, 73 Pa. Stat. §§ 201-1 to 201-9.2 ("UTPCPL")
(On Behalf of Plaintiff, the Nationwide Class and, in the alternative, the Pennsylvania Class)

112. Plaintiff Collins re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

113. Plaintiff Collins and Rutter's are each a "person" as defined at 73 Pa. Stat. § 201-2(2).

114. Plaintiff Collins and Pennsylvania Class Members purchased goods and services in "trade" and "commerce" as defined at 73 Pa. Stat. § 201-2(3).

115. Plaintiff Collins and Pennsylvania Class Members purchased goods and services primarily for personal, family, and/or household purposes under 73 Pa. Stat. § 201-9.2.

116. Rutter's engaged in "unfair methods of competition" or "unfair or deceptive acts or practices" as defined at 73 Pa. Stat. § 201-2(4) by engaging in the following conduct:

(a) Representing that its goods and services had characteristics, uses, benefits, and qualities that they did not have – namely that its goods, services, and business practices were accompanied by adequate data security (73 Pa. Stat. § 201-2(4)(v));

(b) Representing that its goods and services were of a particular standard or quality when they were of another quality (73 Pa. Stat. § 201-2(4)(vii));

(c) Advertising its goods and services with intent not to sell them as advertised (73 Pa. Stat. § 201-2(4)(ix); and

(d) "Engaging in any other . . . deceptive conduct which creates a likelihood of confusion or of misunderstanding" (73 Pa. Stat. § 201-2(4)(xxi)).

117. These unfair methods of competition and unfair or deceptive acts or practices are declared unlawful by 73 Pa. Stat. § 201-3.

118. Rutter's unfair or deceptive acts and practices include but are not limited to: failing to implement and maintain reasonable data security measures to protect Card Information; failing to identify foreseeable data security risks and remediate the identified risks; failing to comply with common law duties, industry standards including PCI DSS, and FTC guidance regarding data security; misrepresenting in its Privacy Policy that it would protect Card Information; and omitting and concealing the material fact that it did not have reasonable measures in place to safeguard Card Information.

119. Rutter's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Rutter's data security practices and ability to protect Card Information.

120. Rutter's intended to mislead consumers and induce them to rely on its misrepresentations and omissions. As set forth herein, Plaintiff did rely on Rutter's misrepresentations and omissions relating to its data privacy and security.

121. Plaintiff Collins and Pennsylvania Class Members acted reasonably in relying on Rutter's misrepresentations and omissions, the truth of which they could not have discovered with reasonable diligence.

122. Had Rutter's disclosed to consumers that its data security systems were not secure and, thus, were vulnerable to attack, Plaintiff Collins and Class Members would not have given their payment data to Rutter's.

123. Rutter's acted intentionally, knowingly, and maliciously in violating the Pennsylvania UTPCPL, and recklessly disregarded consumers' rights.

124. Rutter's past payment card data breaches put it on notice of the importance of data security and that its card processing system was subject to attack.

125. As a direct and proximate result of Rutter's unfair methods of competition and unfair or deceptive acts or practices, Plaintiff Collins and Pennsylvania Class Members have suffered and will continue to suffer damages, injury, ascertainable losses of money or property, and monetary and non-monetary damages as described above.

126. Plaintiff Collins and Pennsylvania Class Members seek all monetary and non-monetary relief allowed by law, including the following as expressly permitted under 73 Pa. Stat. § 201-9.2:

(a) "actual damages or [statutory damages of] one hundred dollars ($100), whichever is greater";

(b) treble damages, defied as "three times the actual damages";

(c) "reasonable attorney fees" and litigation costs; and

(d) "such additional relief as [the Court] deems necessary or proper."

127. Plaintiff Collins and Pennsylvania Class Members also seek the injunctive relief as set forth above.

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiff, the Nationwide Class, and, in the alternative, the Pennsylvania Class)

128. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

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

130. Plaintiff and Class Members conferred a monetary benefit upon Rutter's in the form of monies paid for the purchase of food and food-related services at its locations.

131. Rutter's appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Rutter's also benefited from the receipt of Plaintiff's and Class Members' Card Information, as this was utilized by Rutter's to facilitate payment to it.

132. The monies Plaintiff and Class Members paid to Rutter's were supposed to be used by Rutter's, in part, to pay for adequate data privacy infrastructure, practices, and procedures.

133. As a result of Rutter's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their purchases made with adequate data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those purchases without adequate data privacy and security practices and procedures that they received.

134. Under principals of equity and good conscience, Rutter's should not be permitted to retain the money belonging to Plaintiff and Class Members because Rutter'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.

135. Rutter'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.

RELIEF REQUESTED

Plaintiff, on behalf of all others similarly situated, requests that the Court enter judgment against Rutter's including the following:

A. Determining that this matter may proceed as a class action and certifying the Classes asserted herein;

B. Appointing Plaintiff as representative of the applicable Classes and appointing Plaintiff's counsel as class counsel;

C. An award to Plaintiff and the Classes of compensatory, consequential, statutory, and treble damages as set forth above;

D. Ordering injunctive relief requiring Rutter's to (among other things): (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide several years of free credit monitoring and identity theft insurance to all Class Members;

E. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

F. An award of pre-judgment and post-judgment interest, as provided by law or equity; and

G. Such other relief as the Court may allow.

JURY TRIAL DEMAND

Plaintiff demands a trial by jury trial all issues so triable.

Dated: March 4, 2020

Respectfully submitted,

/s/ Benjamin F. Johns

Benjamin F. Johns (201373)
Mark B. DeSanto (320310) (*pro hac vice* application forthcoming)
CHIMICLES SCHWARTZ KRINER & DONALDSON-SMITH LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041
Tel: (610) 642-8500
bfj@chimicles.com

mbd@chimicles.com

Cornelius P. Dukelow (*pro hac vice* application forthcoming)
Oklahoma Bar No. 19086
ABINGTON COLE + ELLERY
320 South Boston Avenue, Suite 1130
Tulsa, Oklahoma 74103
918.588.3400 (telephone & facsimile)
cdukelow@abingtonlaw.com
www.abingtonlaw.com

Tina Wolfson (*pro hac vice* application forthcoming)
AHDOOT & WOLFSON, PC
10728 Lindbrook Drive
Los Angeles, California 90024
Tel: (310) 474-9111
Fax: (310) 474-8585
twolfson@ahdootwolfson.com

Counsel for Plaintiff and the Classes