PIIN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

JON LAVEZZA, individually and on behalf of all others similarly situated,

Plaintiff,

v.

RUTTER'S HOLDINGS, INC.,

Defendant.

Civil Action No.:

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff, Jon Lavezza ("Plaintiff" or "Mr. Lavezza"), individually and on behalf of all others similarly situated, on personal knowledge of the facts respectively pertaining to himself and on information and belief as to all other matters, by and through his undersigned counsel, hereby brings this Class Action Complaint against Defendant Rutter's Holdings, Inc. ("Rutter's").

I. NATURE OF THE ACTION

1. Plaintiff brings this class action against Rutter's for its failure to exercise reasonable care in securing and safeguarding its customers' Private Information ("Private Information" or "PI"), specifically the credit card information, including cardholder names, credit card numbers, expiration dates, and internal verification codes.

2. Rutter's is a chain of convenience stores and gas stations with 72 locations in Central Pennsylvania, West Virginia, and Maryland. It provides a platform available online and through mobile devices for customers to book and change their travel. Customers are led to believe and agree to provide Private Information based on the fact that Rutter's will safeguard their Private Information and that Rutter's will share the information only with the persons, entities, and groups with whom the customer consents.

3. However, on or about September 6, 2018, Plaintiff and Class members learned that commencing in or around August 2018, their Private Information was stolen from Rutter's database storing Personal Information by hackers as a result of Rutter's security failures. Almost two months after announcement of the initial breach, Rutter's announced that an internal investigation has revealed that the data breach was far greater than originally believed.

4. Rutter's security failures exposed Plaintiff's and Class members' Private Information to a massive security breach affecting hundreds of thousands of customers (the "Security Breach"). The failures put Plaintiff's and Class members' personal and financial information and interests at serious, immediate, and ongoing risk.

5. The Security Breach was caused and enabled by Rutter's knowing violation of its obligations to abide by best practices and industry standards concerning the security of its users' Private Information. Rutter's failed to comply with security standards and allowed its users' Private Information to be compromised by cutting corners on security measures that should have been employed and could have prevented or mitigated the Security Breach that occurred.

II. JURISDICTION AND VENUE

6. The Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

7. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) and 1391(c)(2) because the Plaintiff and many class members reside in this District, Defendant is headquartered within this District, and because Rutter's is subject to personal jurisdiction in Pennsylvania. In addition, the events giving rise to Plaintiff's causes of action arose, in part, in this District.

III. PARTIES

8. Plaintiff Jon Lavezza is a resident of York, Pennsylvania. He regularly has patronized multiple Rutter's locations over the past 18 months, including the Dallastown, North Hills, Loganville, and East Prospect locations.

9. In or around early Fall of 2019, Mr. Lavezza discovered that his checking account was compromised and emptied as a result of unauthorized access. Mr. Lavezza was charged with multiple overdraft fees during this time.

10. Mr. Lavezza did not have access to his checking account funds for several days before his bank could reimburse him, and it took approximately one week for his new debit card to arrive.

11. Mr. Lavezza spent significant time addressing the unauthorized access to his account, including leaving work early one day, missing work time to file a police report, and missing yet another half day of work while talking with the bank. Mr. Lavezza estimates that he lost approximately one full day of work addressing the unauthorized access to this account.

12. Plaintiff is also at risk of imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Private Information being placed in the hands of criminals.

13. Plaintiff has a continuing interest in ensuring that his PI is protected and safeguarded from future breaches.

14. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of his PI—a form of intangible property that Plaintiff entrusted to Defendant that was compromised in and as a result of the Security Breach. Plaintiff also was forced to expend valuable time to rectify the loss of his card and privileges while overseas.

15. The injuries suffered by Plaintiff and Class members as a direct result of the Security Breach include:

a. theft of their personal and financial information;

b. improper disclosure of their PI;

c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PI being placed in the hands of criminals and potential sale of Plaintiff's and Class members' information on the Internet black market;

d. damages to and diminution in value of their PI entrusted to Rutter's and the loss of Plaintiff's and Class members' privacy; and,

e. loss of time from addressing the breach and loss of the value of cancelled credit cards, including loss of rewards points that would have accrued from the time of cards' cancellation until a new card is issued.

16. Defendant Rutter's headquarters is in York, Pennsylvania.

17. Defendant Rutter's is a chain of convenience stores and gas stations with 72 locations in Central Pennsylvania, West Virginia, and Maryland.

IV. FACTUAL BACKGROUND

18. On February 13, 2020, Rutter's posted a "Notice of Credit Card Incident" on its website, which indicated that it had been made aware of a malware intrusion on Rutter's payment processing servers that compromised its payment card environment and customers' sensitive Card Information. The Notice of Credit Card Incident provides the following in pertinent part:

> 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.[1]

19. As confirmed by the Notice of Credit Card Incident, Rutter's believes the Data Breach occurred between as early as August 30, 2018, lasting through May 29, 2019:

> 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.[2]

20. However, neither the Notice of Credit Card Incident, nor any statements issued by Rutter's give any indication as to the actual magnitude of the Data Breach, including confirmation of the exact number of stores impacted or the actual number of customers and cards affected.

21. Although the Notice of Credit Card Incident indicates Rutter's also "notified law enforcement" and engaged cybersecurity firms, it is still unclear what such efforts involve, as Rutter's has not disclosed exactly what was communicated to authorities.

22. Rutter's has long known the critical importance of protecting users' Private Information from unauthorized access. Rutter's also knows the multitude of harms that foreseeably flow to individual users when information is stolen or misused by criminals.

23. It is well known in the retail industry that sensitive PI is valuable and frequently targeted by hackers. In a recent article, Business Insider noted that "[d]ata breaches are on the rise

[1] *See* https://www.rutters.com/paymentcardincident/ (last accessed Mar. 2, 2020).

[2] *Id.*

for all kinds of businesses, including retailers …. Many of them were caused by flaws in payment systems either online or in stores."[3]

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

> 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.[4]

25. Despite the known risk of point-of-sale (POS) malware intrusions and the widespread publicity and industry alerts regarding other notable (similar) data breaches, Rutter'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.

26. Rutter'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.

27. Rutter's explicit statements in its Privacy Policy make clear that Rutter's recognized the importance of adequately safeguarding its customers' PI, yet Rutter's failed to take the steps necessary to protect the sensitive information. On its website, Rutter's privacy policy provides the following:

---

[3] 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, 11:05 a.m.), available at https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1 (last accessed Dec. 16, 2019).

[4] *Cyber Attack on Earl Enterprises (Planet Hollywood)*, is Buzznews (Apr. 1, 2019), available at https://www.informationsecuritybuzz.com/expert-comments/cyber-attack-on-earl-enterprisesplanet-hollywood/ (last accessed Dec. 16, 2019).

> This Privacy Policy covers the data collection practices of Rutter's Dairy and Rutter's Farm Stores, Inc. websites, www.rutters.com and www.ruttersrewards.com, and the Rutter's Rewards mobile app operated by Rutter's Farm Stores, Inc. This Privacy Policy describes our privacy practices and those of our vendors and business partners on the Website.
>
> * * *
>
> 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.[5]

28. The Privacy Policy goes on to explain the types of information collected and how Rutter's may use such information.

29. Rutter's is thus aware of the importance of safeguarding its customers' PI from the foreseeable consequences that would occur if its data security systems and computer servers were breached.

30. 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.

31. As stated above, the customer information taken included: names, billing addresses, email addresses, and credit card information, including credit card numbers, expiry dates and, perhaps most troubling, CVV codes. CVV codes are not to be saved at any time, which means that the hackers were able to take them from live transactions or, alternatively, Rutter's was storing them in violation of well-established security standards.

32. 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

[5] Rutter's "Privacy Policy," available at https://www.rutters.com/privacy-policy/ (last accessed Mar. 2, 2020).

Standards Council. The PCI DSS list applies to all organizations and environments where cardholder data is stored, processed, or transmitted, and requires merchants like Rutter's to protect cardholder data, ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks, and ensure the maintenance of information security policies.

33. 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; and,
12. Maintain a policy that addresses information security for all personnel.[6]

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

35. Had Rutter's followed these PCI DSS requirements, the hackers could not have breached Rutter's systems to steal customer data, particularly the CVV codes.

[6]Payment Card International (PCI) Data Security Standard, "Requirements and Security Assessment Procedures, Version 3.2.1," (May 2018), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1583188243051

36. Rutter'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.

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

38. 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.

39. In 2007, the FTC published guidelines that established 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.

40. In the U.S., the FTC has issued numerous guides for businesses, highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[7]

41. In 2016, the FTC updated its publication, *Protecting Private Information : A Guide for Business*, which establishes guidelines for fundamental data security principles and practices for business.[8] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of Private Information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

42. The FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[9]

43. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an

[7] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited April 4, 2018).

[8] Federal Trade Commission, *Protecting Private Information : A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited April 4, 2018).

[9] Federal Trade Commission, *Start With Security*, *supra* n. 6.

unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

44. Rutter's was at all times fully aware of its obligation to protect the Private Information of its customers. Rutter's also was aware of the significant repercussions if it failed to do so because it collected Private Information to process transactions and knew that this data, if hacked, would result in injury to Plaintiff and Class members.

Security Breaches Lead to Identity Theft

45. According to the U.S. Department of Justice Bureau of Justice Statistics, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014.[10]

46. Similarly, the FTC cautions that identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[11] Identity thieves use stolen Private Information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[12]

47. Private Information is a valuable commodity to identity thieves. Plaintiff's and Class members' Private Information can be sold and traded by cyber criminals on the dark web. Criminals often trade the information on the dark web for a number of years.

[10] *See Victims of Identity Theft, 2014*, DOJ, at 1 (2015), available at https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited September 18, 2018).

[11] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, at 3 (2012), available at http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited September 18, 2018).

[12] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

48. The National Institute of Standards and Technology categorizes the combination of names and credit card numbers as sensitive and warranting a higher impact level based on the potential harm when used in contexts other than their intended use.[13] Private Information that is "linked" or "linkable" is also more sensitive. Linked information is information about or related to an individual that is logically associated with other information about the individual. Linkable information is information about or related to an individual for which there is a possibility of logical association with other information about the individual. An example of linking information the NIST report cites is a Massachusetts Institute of Technology study showing that 97% of the names and addresses on a voting list were identifiable using only ZIP code and date of birth.

49. Private Information is broader in scope than directly identifiable information. As technology advances, computer programs become increasingly able to scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible.

50. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[14] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

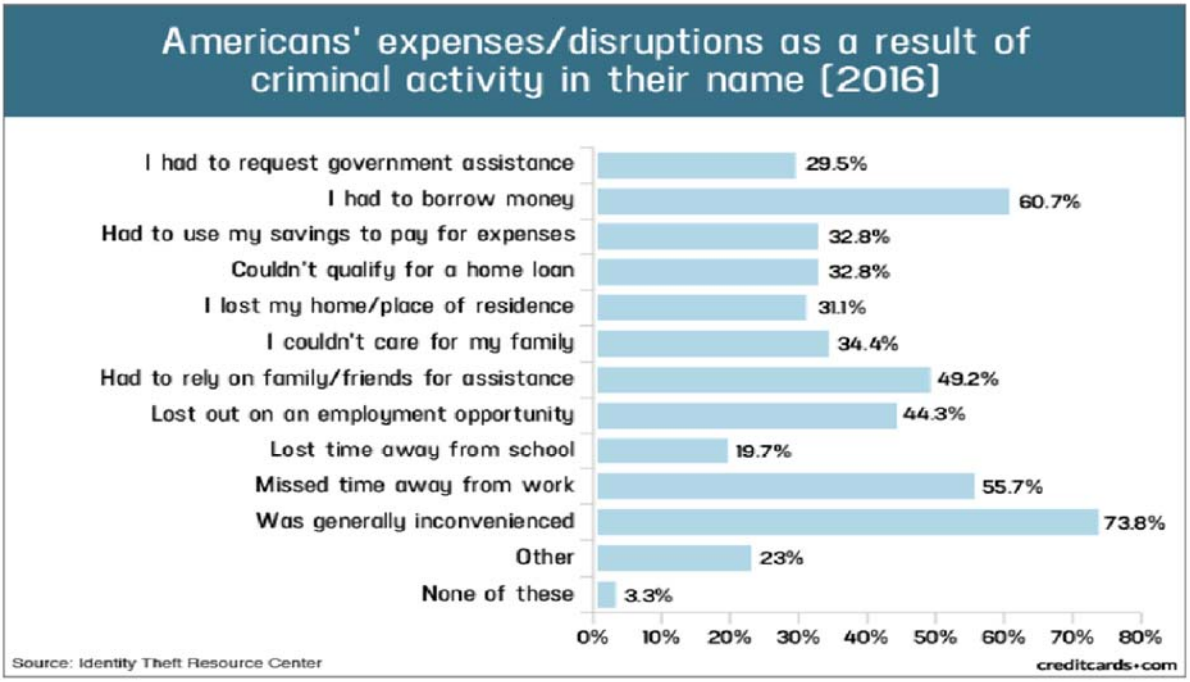
---

[13] Erika McCallister, et al., *Guide to Protecting the Confidentiality of Personally Identifiable Information (PI)*, National Institute of Standards and Technology Special Publication 800-122, 3-3, available at http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=904990 (last visited September 18, 2018).

[14] *Supra,* n.16.

51. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349."[15]

52. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of Private Information :[16]



V. CLASS ACTION ALLEGATIONS

53. Plaintiff brings all counts, as set forth below, on behalf of himself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a Nationwide Class defined as:

[15] *See* Department of Justice, *Victims of Identity Theft, 2014*, *supra* n. 11 at 6 .

[16] Source: "Credit Card and ID Theft Statistics" by Jason Steele, available at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited September 18, 2018).

> All persons in the United States who paid for items via credit card at Rutter's from August 30, 2018 through May 29, 2019: (the "Nationwide Class").

54. In the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims under the laws of the State of Pennsylvania and on behalf of the Pennsylvania Subclass, defined as follows:

> All persons in the Commonwealth of Pennsylvania who paid for items via credit card at Rutter's from August 30, 2018 through May 29, 2019: (the "Pennsylvania Class").

55. Excluded from the Class and Subclass are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

56. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

57. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class and Subclass are so numerous that joinder of all Class members would be impracticable. On information and belief, Class and Subclass members number in the thousands.

58. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class and Subclass members and predominate over questions affecting only individual Class and Subclass members. Such common questions of law or fact include, *inter alia*:

a. Whether Rutter's failed to use reasonable care and commercially reasonable methods to secure and safeguard Plaintiff's and Class and Subclass members' Private Information;

b. Whether Rutter's properly implemented its purported security measures to protect Plaintiff's and Class and Subclass members' Private Information from unauthorized capture, dissemination, and misuse;

c. Whether Rutter's took reasonable measures to determine the extent of the Security Breach after it first learned of same;

d. Whether Rutter's conduct constitutes breach of an implied contract;

e. Whether Rutter's willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and Class and Subclass members' Private Information;

f. Whether Rutter's was negligent in failing to properly secure and protect Plaintiff's and Class and Subclass members' Private Information;

g. Whether Plaintiff and the other members of the Class and Subclass are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief;

h. Whether Rutter's engaged in conduct in violation of 73 Pa. Stat. §§ 201-1 to 201-9.2 by its conduct; and,

i. Whether Plaintiff, Class, and Subclass are entitled to statutory damages.

59. Rutter's engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of himself and other Class and Subclass members. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

60. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other Class and Subclass members because, among other things, all Class members were similarly injured through Rutter's uniform misconduct described above and were thus all subject to the Security Breach alleged herein. Further, there are no defenses available to Rutter's that are unique to Plaintiff.

61. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate Class and Subclass representative because his interests do not conflict with the interests of the other Class and Subclass members he seeks to represent, he has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The Class' and Subclass' interests will be fairly and adequately protected by Plaintiff and his counsel.

62. **Insufficiency of Separate Actions—Federal Rule of Civil Procedure 23(b)(1).** Absent a representative class action, members of the Class and Subclass would continue to suffer the harm described herein, for which they would have no remedy. Even if separate actions could be brought by individual consumers, the resulting multiplicity of lawsuits would cause undue hardship and expense for both the Court and the litigants, as well as create a risk of inconsistent rulings and adjudications that might be dispositive of the interests of similarly situated consumers, substantially impeding their ability to protect their interests, while establishing incompatible standards of conduct for Rutter's. The Class and Subclass thus satisfy the requirements of Fed. R. Civ. P. 23(b)(1).

63. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or

other financial detriment suffered by Plaintiff and the other Class and Subclass members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Rutter's, so it would be impracticable for Class members to individually seek redress for Rutter's wrongful conduct. Even if Class and Subclass members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

64. In the alternative, to certification pursuant to Rule 23(b)(3), Plaintiff submits that certification is proper as to certain issues pursuant to Rule 23(c)(4).

VI. CAUSES OF ACTION

COUNT I

(Negligence)
(On Behalf of Plaintiff and the Nationwide Class, or, Alternatively, Plaintiff and the Pennsylvania Subclass)

65. Plaintiff repeats and realleges the allegations contained in the foregoing paragraphs as though fully set forth herein.

66. Rutter's owes numerous duties to Plaintiff and the other members of the Class. These include duties:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. to protect Private Information in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and,

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and the other members of the Class of the Security Breach.

67. Rutter's knew or should have known the risks of collecting and storing Private Information and the importance of maintaining secure systems. Rutter's own Privacy Security Representations demonstrate it is well aware of these risks and its duty to implement adequate security systems protocols and practices.

68. Rutter's knew or should have known that its security practices did not adequately safeguard Plaintiff's and the other Class members' Private Information.

69. Rutter's breached the duties it owes to Plaintiff and Class members in at least the following ways:

a. By failing to implement adequate security systems, protocols and practices sufficient to protect Rutter's users' Private Information and thereby creating a foreseeable risk of harm;

b. By failing to comply with the minimum industry data security standards during the period of the Security Breach; and,

c. By failing to timely and accurately disclose to Rutter's users that their Private Information had been improperly acquired or accessed.

70. Rutter's further had a duty not to violate the legal rights of any consumer through the employment of unfair or deceptive trade or business practices and had a duty to comply with all provisions of Section 5 of the FTCA, 15 U.S.C. § 45, *et seq.*, as well as 73 Pa. Stat. §§ 201-1 to 201-9.2, *et seq.*

71. The above noted statutes and regulations are designed and intended to protect the interests of persons such as Plaintiff and Class Members.

72. The above noted statutes and regulations are designed and intended to protect persons such as Plaintiff and Class Members from the hazards they encountered and the harm they suffered, including identity theft, as a result of providing their Private Information to Rutter's.

73. The above noted regulations are designed and intended to provide a standard of care by which retail establishments such as Rutter's should operate.

74. Rutter's negligently violated the above statutes and regulations in at least the following ways:

a. By failing to employ reasonable measures to protect consumer PI and failing to comply with applicable industry and regulatory standards, including PCI DSS and FTC guidance, as set forth above, despite the readily foreseeable consequences of a data breach and the amount of consumer PI that Rutter's retained, as pled herein; and,

b. By falsely representing that adequate measures to protect consumer PI were in place, being aware that consumers would reasonably rely on those measures being in place in order to transact with the use of credit cards, as pled herein.

75. Rutter's failure to comply with the above noted regulations constitutes negligence *per se*.

76. But for Rutter's wrongful and negligent breach of the duties it owed to Plaintiff and the other Class members, as set forth above, their Private Information would not have been compromised.

77. The injury and harm that Plaintiff and the other Class members suffered were the direct and proximate result of Rutter's negligent conduct.

COUNT II

(Breach of Contract)
(On Behalf of Plaintiff and the Nationwide Class, or, Alternatively, Plaintiff and the Pennsylvania Subclass)

78. Plaintiff repeats and realleges the allegations contained in the foregoing paragraphs as though fully set forth herein.

79. By providing their Personal Information, credit card information, as a medium of payment, in exchange for Rutter's products and services, Plaintiff and Class Members entered into an implied contract with Rutter's, wherein Rutter's agreed to take reasonable steps to protect the Credit Card Information and PI.

80. As part of their regular business practices, Rutter's invited Plaintiff and Class Members to provide their PI to facilitate payment for Rutter's products and services. Plaintiff and Class members accepted Rutter's offer and, thus, provided such information.

81. When entering into implied contracts with Rutter's, Plaintiff and Class Members reasonably believed that Rutter's would employ data security measures that were up to industry standards and compliant will all relevant laws and regulations.

82. Rutter's implied promise to keep customer PI safe is evidenced by the representations in its Privacy Policy and its notice to consumers that followed the data breach, as set forth above.

83. Rutter's was aware of the obvious harm that would result to Plaintiff and Class Members if it failed to adequately secure the PI of Plaintiff and Class Members.

84. When Plaintiff and Class Members paid money to Rutter's to purchase items at Rutter's stores and gas pumps, they reasonably believed that Rutter's would use some of those funds to provide adequate data security.

85. In the absence of a promise to safeguard PI, and keep it reasonably secure, Plaintiff and Class Members would not have given their information to Rutter's.

86. By paying for their purchased goods and services, Plaintiff and Class Members fully performed on their implied contract with Rutter's.

87. By failing to implement reasonably adequate security measures, Rutter's breached a material term of its implied contract with Plaintiff and Class Members.

88. As a direct and proximate result of Rutter's breaches of contract, Plaintiff and Class Members suffered the damages as alleged herein.

89. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the data breach.

90. Plaintiff and Class Members are further entitled to injunctive relief, requiring Rutter's to strengthen its data security systems and monitoring procedures, submit to future audits of those systems, and provide several years of credit monitoring and identity theft protection to all Class Members.

COUNT III

(Violations of the Pennsylvania Unfair Trade Practices and Consumer Protection Law) (73 Pa. Stat. §§ 201-1 to 201-9.2)

(On Behalf of Plaintiff and the Nationwide Class, or, Alternatively, Plaintiff and the Pennsylvania Subclass)

91. Plaintiff repeats and realleges the allegations contained in the foregoing paragraphs as though fully set forth herein.

92. Plaintiff, Class Members, and Rutter's are all "persons" as that term is defined 73 Pa. Stat. § 201-2(2).

93. Plaintiff and Class Members purchased good and services in trade and commerce, as defined by 73 Pa. Stat. § 201-2(3).

94. Plaintiff and Class Members purchased these goods and services for personal, family, and/or household use as comprehended by 73 Pa. Stat. § 201-9.2.

95. Rutter's engaged in "unfair methods of competition" and/or "unfair or deceptive acts or practices," as defined by 73 Pa. Stat. § 201-2(4), by:

a. Representing that Rutter's goods and services had characteristics, uses, benefits, and qualities that they did not have, these characteristics and qualities being adequate data protection for credit card purchasers and consumer PI, in violation of 73 Pa. Stat. § 201-2(4)(v), as pled herein;

b. Representing that Rutter's goods and services were of a particular standard or quality when they were of an inferior quality, in violation of 73 Pa. Stat. § 201-2(4)(vii), as pled herein;

c. Advertising goods and services with the intent not to sell them as advertised, in violation of 73 Pa. Stat. § 201-2(3)(ix), as pled herein; and,

d. Engaging in deceptive conduct that creates a likelihood of confusion or misunderstanding for consumers, by inviting Rutter's customers to purchase goods and services with credit cards, creating the false impression that it is safe to do so, in violation of 73 Pa. Stat. § 201-2(4)(xxi), as pled herein.

96. Pursuant to 73 Pa. Stat. § 201-3, these unfair methods of competition and unfair or deceptive acts or practices are unlawful.

97. Rutter's unfair or deceptive acts and business practices include, but are not limited to, at least the following:

a. The failure to implement and maintain adequate data security measures to protect consumer PI;

b. The failure to identify reasonably foreseeable defects in their data security system and take adequate steps to repair them;

c. The failure to comply with all relevant and applicable industrial, legal, and regulatory standards for data security, including PCI DSS and FTC guidance;

d. Making false and deceptive statements that Rutter's would adequately protect consumer PI, as detailed in their Privacy Policy; and,

e. Omitting and concealing the material fact that Rutter's did not have adequate or reasonable security measures in place to protect consumer PI.

98. Rutter's made material representations regarding the adequacy of its data security practices and ability to protect Credit Card Information, that were likely to deceive reasonable consumers.

99. Rutter's intended to mislead consumers and induced them to rely on its misrepresentations and omissions. Further, Plaintiff and Class Members did rely on Rutter's misrepresentations and omissions, relating to the adequacy of its data security practices and ability to protect Credit Card Information, as set forth herein.

100. Plaintiff and Class Members could not have discovered the truth of Rutter's misrepresentations and omissions with the use of reasonable diligence and acted reasonably by relying on such misrepresentations and omissions.

101. If Rutter's had disclosed the fact that its data security systems were insecure and vulnerable to attack, Plaintiff and Class Members would not have entrusted Rutter's with their Credit Card Information.

102. Rutter's intentionally, knowingly, and maliciously violated the Pennsylvania UTPCPL, in reckless disregard of consumers' rights.

103. Rutter's was aware of the importance of data security, and on notice that its card processing system was vulnerable to attack, due to its own prior security breaches, as well as the highly publicized attacks on other retailers nationwide.

104. As a direct and proximate result of Rutter's unfair methods of competition and unfair or deceptive acts and/or practices, Plaintiff and 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.

105. In addition to the injunctive relief set forth above, Plaintiff and Class Members seek the following relief, Pursuant to 73 Pa. Stat. § 201-9.2:

a. The greater of actual damages or statutory damages of one hundred dollars ($100);

b. Reasonable attorneys' fees and litigation costs; and,

c. Such additional monetary or non-monetary relief as this Honorable Court deems proper.

VII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all claims so triable.

VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in his favor and against Rutter's, as follows:

A. Declaring that this action is a proper class action, certifying the Class and Subclass as requested herein, designating Plaintiff as Class and Subclass Representative, and appointing Class Counsel as requested in Plaintiff's motion for class certification;

B. Ordering Rutter's to pay actual damages to Plaintiff and the other members of the Class and Subclass;

C. Ordering Rutter's to pay attorneys' fees and litigation costs to Plaintiff, the Class, and their counsel;

D. Ordering Rutter's to pay equitable relief, in the form of disgorgement and restitution, as may be appropriate;

E. Ordering Rutter's to pay both pre- and post-judgment interest on any amounts awarded; and,

F. Ordering such other and further relief as may be just and proper.

Date: March 25, 2020

Respectfully submitted,

/s/ D. Aaron Rihn

D. Aaron Rihn, Esquire
PA I.D. No.: 85752
ROBERT PEIRCE & ASSSOCIATES, P.C.
707 Grant Street, Suite 125
Pittsburgh, PA 15219
Tel: 412-281-7229

Fax: 412-281-4229
arihn@peircelaw.com

Nicholas A. Migliaccio, Esquire*
Jason S. Rathod, Esquire*
MIGLIACCIO & RATHOD LLP
412 H Street NE, Suite 302
Washington, DC 20002
Tel: 202-470-3520
nmigliaccio@classlawdc.com
jrathod@classlawdc.com

Attorneys for Plaintiff and the Putative Class and Subclass

* admission to be sought

JS 44 (Rev. 02/19)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS
Jon Lavezza, Individually and on behalf of all others similarly situated,

DEFENDANTS
Rutter's Holdings, Inc.

(b) County of Residence of First Listed Plaintiff York
(EXCEPT IN U.S. PLAINTIFF CASES)

County of Residence of First Listed Defendant York
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Robert Peirce & Associates, PC
707 Grant Street, Suite 125
Pittsburgh, PA 15219

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☒ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*
Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☒ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION
Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. Section 1332(d)
Brief description of cause:
Data Breach

VII. REQUESTED IN COMPLAINT:
☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.
DEMAND $ 5,000,100.00
CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY *(See instructions):*
JUDGE _____ DOCKET NUMBER _____

DATE 03/25/2020
SIGNATURE OF ATTORNEY OF RECORD /s/ D. Aaron Rihn

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____