UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF CONNECTICUT

MARK JONES, Individually and on Behalf of All Others Similarly Situated,	**Civil Action No.:**
Plaintiff,	**CLASS ACTION COMPLAINT**
v.	**JURY TRIAL DEMANDED**
STURM, RUGER & COMPANY, INC.,	**Date: October 4, 2022**
Defendant.	

Plaintiff Mark Jones, individually and on behalf of all others similarly situated, brings this Class Action Complaint ("Complaint") against Defendant Sturm, Ruger & Company, Inc. ("Ruger" or "Defendant"), a Connecticut corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, which are made on personal knowledge, the investigation of his counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of the recent data breach ("Data Breach") involving Sturm, Ruger & Company, Inc., a firearms design, manufacturing, and sales company headquartered in Southport, Connecticut.

2. Ruger owns the website www.ShopRuger.com ("ShopRuger.com") where it sells certain products and merchandise directly to consumers. To make a purchase or register an account on ShopRuger.com, Plaintiff and Class Members were required to provide certain sensitive, non-public information to Defendant. Unfortunately, Ruger failed to properly secure and safeguard the personally identifiable information provided by customers when making purchases on this website,

including without limitation, their unencrypted and unredacted first and last names, shipping addresses, and email addresses ("PII"), their payment card data which includes their credit/debit card numbers in combination with security codes, access codes, card expiration dates, and billing addresses ("PCD"), and other sensitive information including the product they purchased, the price they paid, and the number of items purchased (collectively with PII and PCD, "Private Information").

3. On information and belief, this Data Breach was engineered and targeted at accessing and exfiltrating the Private Information of Plaintiff and Class Members in order for criminals to use that information in furtherance of theft, identity crimes, and fraud.

4. Defendant's failure to prevent and detect the Data Breach is particularly egregious considering the nature of its business and the Private Information it collected. The aggregate information acquired by cybercriminals in this Data Breach is particularly concerning considering that Defendant's customers were purchasing firearm accessories from ShopRuger.com. Criminals can now access their Private Information which includes the nature of their purchases and their shipping and billing addresses. With this information criminals can target the homes of firearm owners to steal firearms that they cannot obtain through legal channels.

5. Plaintiff brings this class action against Ruger to seek damages for himself and other similarly situated consumers impacted by the Data Breach ("Class Members"), as well as other equitable relief, including, without limitation, injunctive relief designed to protect the sensitive information of Plaintiff and other Class Members from further data breach incidents.

6. In a letter dated August 18, 2022, Ruger notified various state Attorneys General, as well as Plaintiff and Class Members, that Freestyle Solutions, its third-party vendor (and agent) that hosts Ruger's e-commerce website, www.ShopRuger.com, had sustained a data breach (the

"Notice Letter"). According to the Notice Letter, between September 18, 2020, and February 3, 2022, malware infected the Freestyle Solutions' server that housed the ShopRuger.com website, allowing the PII and PCD of Plaintiff and Class Members to be captured and compromised by data thieves.[1]

7. As a result of Defendant's failure to prevent the Data Breach, or detect it during the nearly two years that criminals were siphoning its customers' personal and private data, thousands of ShopRuger.com customers across the United States have suffered real and imminent harm as a direct consequence of Defendant's conduct, which includes: (a) refusing to take adequate and reasonable measures to ensure its data systems were protected; (b) refusing to take available steps to prevent the breach from happening; (c) failing to adequately audit and monitor its third party data security vendors; (d) failing to disclose to its customers the material fact that it or its vendors did not have adequate computer systems and security practices to safeguard customers' personal and financial information; and (e) failing to provide timely and adequate notice of the data breach.

8. The injuries suffered by Plaintiff and Class Members as a direct result of the Data Breach include, *inter alia*:

a. Unauthorized charges on their payment card accounts;

b. Theft of their personal and financial information;

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

d. Loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the

[1] *Sturm Ruger & Company Data Breach Notice to Consumers*, OFF. VT. ATT'Y GEN. (Aug. 16, 2022), https://ago.vermont.gov/blog/2022/08/16/sturm-ruger-company-data-breach-notice-to-consumers/.

amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit, including decreased credit scores and adverse credit notations;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempting to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the data breach;

f. The imminent and certainly impending injury flowing from potential theft, fraud, and identity theft posed by their Private Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted to Ruger for the sole purpose of making purchases from Ruger and with the mutual understanding that Ruger would safeguard Plaintiff's and Class Members' Private Information against theft and not allow access to and misuse of their information by others;

h. Money paid to Ruger during the period of the Data Breach in that Plaintiff and Class Members would not have purchased from Ruger, or would have paid less for their purchases, had Defendant disclosed that it lacked adequate systems and procedures to reasonably safeguard customers'

Private Information and had Plaintiff and Class Members known that Ruger would not provide timely and accurate notice of the Data Breach; and,

i. Continued risk to their PII and PCD, which remains in the possession of Ruger and its vendors, and which is subject to further breaches so long as Ruger continues to fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data in its possession.

9. Examples of the harms to Ruger customers as a direct and foreseeable consequence of its conduct include the experiences of the representative Plaintiff, which are described below.

THE PARTIES

Plaintiff Mark Jones

10. Plaintiff Mark Jones is a citizen of the State of Ohio and a is a resident of Sydney, Ohio.

Defendant Ruger

11. Defendant is a publicly traded corporation incorporated in the State of Delaware. Defendant's headquarters is located at 1 Lacey Place, Southport, Connecticut 06890. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION & VENUE

12. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. §1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

13. The District of Connecticut has personal jurisdiction over Defendant because Defendant and/or its parents or affiliates are headquartered in this District and Defendant conducts substantial business in Connecticut and this District through its headquarters, offices, parents, and affiliates.

14. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Background

15. Ruger is primarily engaged in the design, manufacture, and sale of firearms to its customers located within the United States. Ruger is a publicly traded company with corporate headquarters in Southport, Connecticut. As of February 1, 2022, Ruger employed approximately 1,912 full-time employees.[2]

16. Ruger operates a consumer facing website, ShopRuger.com, located at www.shopruger.com. On its website, Ruger sells a variety of firearm accessories, knives and tools, pepper spray, cleaning supplies, shooting supplies, safety equipment, survival gear, hunting gear, as well as other types of sporting accessories and apparel, direct to retail purchasers.[3]

17. To make a purchase on ShopRuger.com a customer must provide certain PII and PCD, including, but not limited to, the customer's name, mailing address, e-mail address, phone number, and credit or debit card number, etc.[4]

---

[2] Sturm Ruger & Co. Inc., Annual Report, (Form 10-K) (Feb. 23, 2022), https://sec.report/Document/0001174947-22-000269/.

[3] *See* Sturm Ruger & Co. Inc., https://shopruger.com/# (last visited Sept. 30, 2022).

[4] *Privacy Policy*, https://shopruger.com/privacy.asp (last visited September 20, 2022).

18. In addition to selling merchandise, Ruger requests that its customers provide PII and PCD so that Ruger can register the customer with ShopRuger.com in order to send customers their newsletter and promotions, provide certain other services, and so that it may continue to correspond with the customers.[5]

19. When they provided their Private Information to Defendant, Plaintiff and Class Members relied on Defendant (a large, sophisticated internet retailer) to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

20. Defendant had a duty to take reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to unauthorized third parties. This duty is inherent in the nature of the exchange of the highly sensitive PII and PCD at issue here, particularly where digital transactions are involved.

21. Defendant also recognized and voluntarily adopted additional duties to protect PII and PCD in its Privacy Policy ("Privacy Policy"), which has been publicly posted to the internet.[6] In its Privacy Policy, Ruger also promises that it takes "commercially reasonable steps to help protect and secure the Personal Information we collect," and further promises that, with certain exceptions, "Sturm, Ruger will not disclose to others any of your Personal Information unless we have your express permission."[7]

22. Despite these duties and promises, Ruger allowed data thieves to infect and infiltrate its ShopRuger.com website and steal the Private Information of thousands of its customers.

---

5 *Id.*

6 *Id.*

7 *Id.*

The Data Breach was foreseeable

23. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[8]

24. In light of recent high profile data breaches at other industry leading companies, including Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the Private Information that it collected and maintained would be targeted by cybercriminals.

25. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

26. Despite the prevalence of public announcements of data breach and data security compromises, and despite their own acknowledgment of its duties to keep Private Information confidential and secure, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and the Class from being compromised.

[8] Bree Fowler, *Data breaches break record in 2021*, CNET (Jan. 24, 2022), https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/#:~:text=The%20number%20of%20reported%20data%20breaches%20jumped%2068%20percent%20last,of%201%2C506%20set%20in%202017..

The Data Breach

27. In the Notice Letter, dated August 18, 2022, Ruger notified various state Attorneys General, as well as Plaintiff and Class Members, that its third-party software vendor, Freestyle Solutions, that owns and manages the server hosting ShopRuger.com, had experienced a data breach where the Private Information of certain Ruger customers was "captured and potentially accessed by an unauthorized party."[9]

28. The Notice Letter informed Plaintiff and Class Members that, "On August 2, 2022, Freestyle notified [Ruger] that malware it identified on the Freestyle server hosting the ShopRuger website captured your information."[10]

29. The Private Information exfiltrated in the Data Breach was unencrypted and captured directly from the checkout page at ShopRuger.com.[11]

30. Incredibly, the malicious malware infected ShopRuger.com for a period of nearly 17 months, from September 18, 2020 through February 3, 2022.[12]

31. Despite the incredible risks faced by Plaintiff and Class Members as a result of the Data Breach, Defendant waited until August 18, 2022 to begin mailing notification letters, over seven months after Freestyle Solutions purportedly removed the infected malware from its servers.

32. Despite Defendant's promises that it: (i) would not disclose consumers' Private Information to unauthorized third parties; and (ii) would protect consumers' Private Information with adequate security measures, it appears that Ruger did not even implement, or require its third-party vendors to implement, basic security measures such as immediately encrypting PCD. As

---

9 *Supra*, note 1.

10 *Id*.

11 *Id*.

12 *Id.*

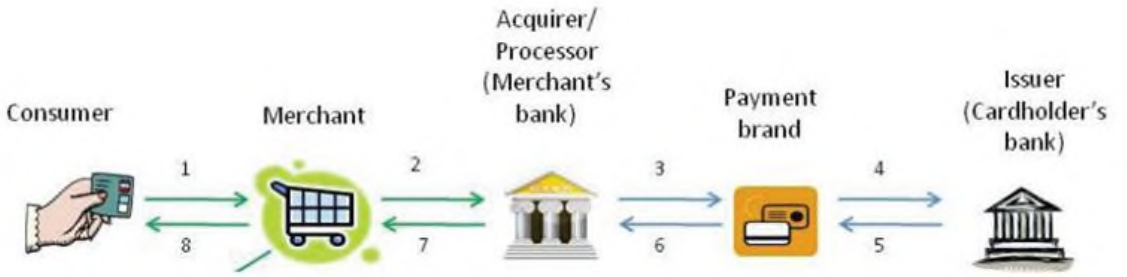
Defendant admits in its Notice Letter, the Private Information "was captured when a customer clicked the 'submission' button on the checkout form, immediately before the data was encrypted and stored . . . ."[13] Ruger also failed to implement adequate regular security reviews or audits of its website, or the servers and networks of its third-party vendors that would have alerted it to the presence of malware sooner than the approximately 17 months it remained undetected.

Securing PII and Preventing Breaches

33. In a debit or credit card purchase transaction, card data must flow through multiple systems and parties to be processed. Generally, the cardholder presents a credit or debit card to an e-commerce retailer (through an e-commerce website) to pay for merchandise. The card is then "swiped," and information about the card and the purchase is stored in the retailer's computers and then transmitted to the acquirer or processor (*i.e.*, the retailer's bank). The acquirer relays the transaction information to the payment card company, who then sends the information to the issuer (*i.e.*, cardholder's bank). The issuer then notifies the payment card company of its decision to authorize or reject the transaction. See graphic below:[14]

[13] *Supra*, note 1.

[14] *Payments 101: Credit and Debit Card Payments*, FIRST DATA, at 7 (Oct. 2010), http://euro.ecom.cmu.edu/resources/elibrary/epay/Payments-101.pdf.



1	The consumer selects a card for payment. The cardholder data is entered into the merchant's payment system, which could be the point-of-sale (POS) terminal/software or an e-commerce website.
2	The card data is sent to an acquirer/payment processor, whose job it is to route the data through the payments system for processing. With e-commerce transactions, a "gateway" provider may provide the link from the merchant's website to the acquirer.
3	The acquirer/processor sends the data to the payment brand (e.g. Visa, MasterCard, American Express, etc.) who forward it to the issuing bank/issusing bank processor
4	The issuing bank/processor verifies that the card is legitimate, not reported lost or stolen, and that the account has the appropriate amount of credit/funds available to pay for the transaction.
5	If so, the issuer generates an authorization number and routes this number back to the card brand. With the authorization, the issuing bank agrees to fund the purchase on the consumer's behalf.
6	The card brand forwards the authorization code back to the acquirer/processor.
7	The acquirer/processor sends the authorization code back to the merchant.
8	The merchant concludes the sale with the customer.

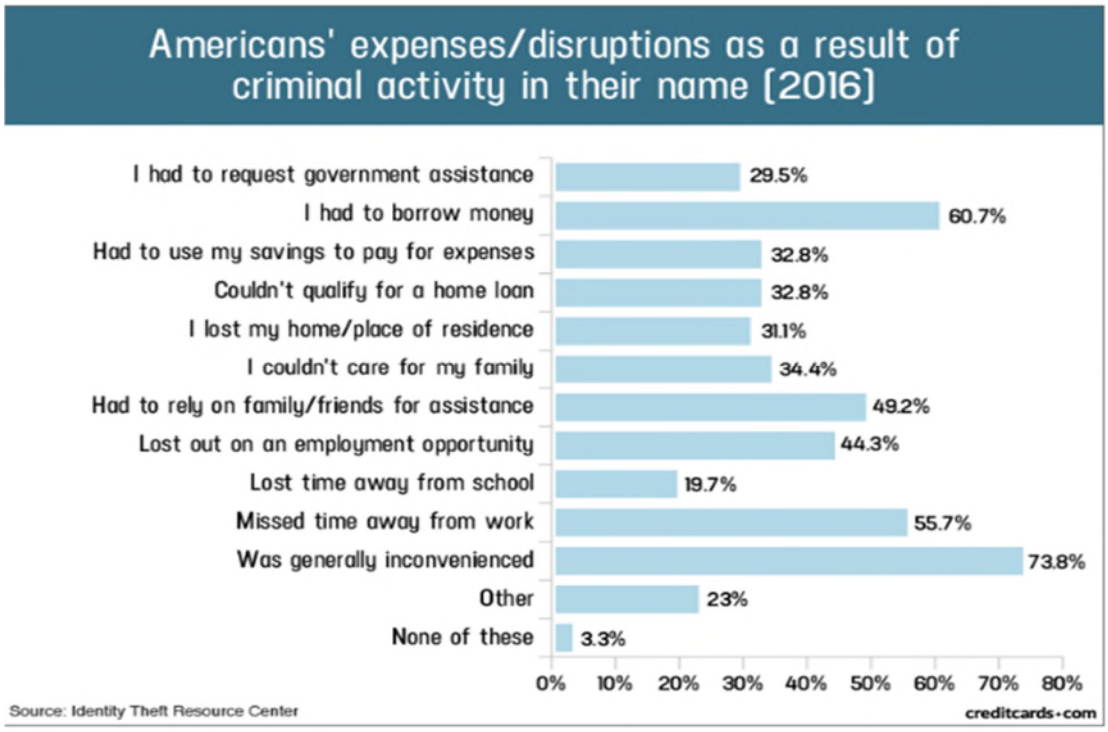
34. There are two points in the payment process where sensitive cardholder data is at risk of being exposed or stolen: pre-authorization when the merchant has captured a consumer's data and it is waiting to be sent to the acquirer; and post-authorization when cardholder data has been sent back to the merchant with the authorization response from the acquirer, and it is placed into some form of storage in the merchant's servers.

35. Encryption mitigates security weaknesses that exist when cardholder data has been stored, but not yet authorized, by using algorithmic schemes to transform plain text information into a non-readable format called "ciphertext." By scrambling the payment card data the moment it is "swiped," hackers who steal the data are left with useless, unreadable text in the place of payment card numbers accompanying the cardholder's personal information stored in the retailer's computers.

36. The financial fraud suffered by Plaintiff and other customers demonstrates that Ruger, and/or its third party vendors, chose not to invest in the technology to encrypt payment card data (PCD) at point-of-sale to make its customers' data more secure; failed to install updates, patches, and malware protection or to install them in a timely manner to protect against a data security breach; and/or failed to provide sufficient control of employee credentials and access to computer systems to prevent a security breach and/or theft of PCD.

37. These failures demonstrate a clear breach of the Payment Card Industry Data Security Standards (PCI DSS), which are industry-wide standards for any organization that handles PCD.

38. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of Private Information:[15]



[15] Jason Steele, *Credit card fraud and ID theft statistics*, CREDITCARDS.COM (June 11, 2021), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited October 27, 2020) [https://web.archive.org/web/20200918073034/https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/].

39. Plaintiff and Class Members have experienced one or more of these harms as a result of the data breach.

40. What's more, theft of Private Information is also gravely serious. Private Information is a valuable property right. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

41. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when PII or PCD is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[16]

42. Private Information and PCD are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

43. There is a strong probability that entire batches of stolen payment card information have been dumped on the black market or are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts for many years to come.

---

[16] U.S. Gov't Accountability Off., GAO 07737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However the Full Extent Is Unknown, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

44. Plaintiff and Class Members have and will continue to suffer injuries as a direct result of the Data Breach. In addition to fraudulent charges and damage to their credit, many victims spent substantial time and expense relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Removing withdrawal and purchase limits on compromised accounts;

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. Spending time on the phone with or at the financial institution to dispute fraudulent charges;

h. Resetting automatic billing instructions; and

i. Paying late fees and declined payment fees imposed as a result of failed automatic payments.

45. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

46. Plaintiff's Private Information was compromised as a direct and proximate result of the Data Breach, and subsequently used for a fraudulent transaction.

47. As a direct and proximate result of the Data Breach, Plaintiff's PII and PCD was "skimmed" and exfiltrated and is in the hands of identity thieves and criminals, as evidenced by the fraud perpetrated against Plaintiff described above.

48. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered actual fraud.

49. As a direct and proximate result of Ruger's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud. Plaintiff and Class Members now have to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

50. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

51. Plaintiff and Class Members also suffered a loss of value of their PII and PCD when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

52. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. The implied contractual bargain entered into between Plaintiff and Ruger included Defendant's contractual obligation to provide adequate data security, which Defendant failed to provide. Thus, Plaintiff and the Class Members did not get what they paid for.

53. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

54. Plaintiff and Class Members have suffered, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. Trespass, damage to and theft of their personal property including PII and PCD;

b. Improper disclosure of their PII and PCD property;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by customers' Private Information being placed in the hands of criminals;

d. Damages flowing from Ruger's untimely and inadequate notification of the Data Breach;

e. Loss of privacy suffered as a result of the Data Breach;

f. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. Ascertainable losses in the form of deprivation of the value of customers' Private Information for which there is a well-established and quantifiable national and international market; and,

h. The loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money customers were permitted to obtain from their accounts.

55. The substantial delay in providing notice of the Data Breach deprived Plaintiff and the Class Members of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach. As a result of Defendant's delay in detecting and notifying consumers of

the Data Breach, the risk of fraud for Plaintiff and Class Members was and has been driven even higher.

Value of Personal Identifiable Information

56. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[17] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[18] Criminals can also purchase access to entire company data breaches from $900 to $4,500.

57. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[19] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[20, 21] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[22]

58. As a result of the Data Breach, Plaintiff's and Class Members' Private Information,

---

[17] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[18] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[19] David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak*, LOS ANGELES TIMES (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[20] See Data Coup, https://datacoup.com/.

[21] *What is digi.me?*, *DIGI.ME*, https://digi.me/what-is-digime/ (last accessed Sept. 30, 2022).

[22] *Frequently Asked Questions*, Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last accessed Sept. 30, 2022).

which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its acquisition by cybercriminals. This transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is likely readily available to others, and the rarity of the Private Information has been destroyed, thereby causing additional loss of value.

59. The fraudulent activity resulting from the Data Breach may not come to light for years and Plaintiff and Class Members face a lifetime risk of fraud and identity theft as a result of the Data Breach.

60. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[23]

61. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, particularly given the sensitive nature of their purchases, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs and risks that would be imposed on Plaintiff and Class Members as a result of a breach.

62. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

---

[23] *Supra*, note 16.

63. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's storage platform, amounting to tens or hundreds of thousands of individuals' detailed, Private Information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

64. To date, Defendant has offered Plaintiff and Class Members only 12 months of identity theft detection services. The offered service is wholly inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the Private Information at issue here.

65. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures, and failure to adequately investigate, monitor, and audit its third-party vendors, to protect the Private Information of Plaintiff and Class Members.

PLAINTIFF JONES' EXPERIENCE

66. Between the period September 18, 2020, and February 3, 2022, Plaintiff visited Ruger's website and provided Ruger with his PII and PCD by using his Discovery credit card in connection with purchases on ShopRuger.com.

67. As required to complete his purchases, Plaintiff provided his Private Information to Ruger on ShopRuger.com. Specifically, during the period of the Data Breach, Plaintiff attempted to purchase several items using his Discover credit card.

68. Subsequent to completing his purchase transaction, Plaintiff was notified by Ruger that his purchased items were not in stock. After waiting several months, Plaintiff's purchased items were cancelled, but Ruger retained possession of Plaintiff's PII and PCD.

69. After his transaction on Defendant's website, Plaintiff experienced five fraudulent purchases on his Discover credit card.

70. Plaintiff was forced to spend time cancelling his compromised Discover credit card and having a new one issued to prevent further fraudulent charges.

71. Plaintiff received a Notice Letter from Ruger dated August 18, 2022, informing him that Freestyle Solutions, the third-party vendor that owned and managed the server hosting ShopRuger.com, had sustained a data breach and that Plaintiff's Private Information was captured and compromised.

72. The Notice Letter from Ruger informed Plaintiff that unauthorized individuals may have gained access to his Private Information when he completed his transactions on ShopRuger.com.

73. As a result of the fraudulent charges on Plaintiff's Discover Card, Plaintiff was forced to spend time corresponding with his credit card issuer to address the fraudulent charges.

74. Plaintiff suffered actual injury in the form of time spent dealing with fraud resulting from the Data Breach and/or monitoring his accounts for fraud.

75. Plaintiff suffered actual injury in the form of fraudulent charges on his Discover credit card and the loss of use of funds while disputing the unauthorized charge and additional damages resulting from such loss of use.

76. Plaintiff was not reimbursed for the loss of use of, loss of access to, or restrictions placed upon his account and the resulting loss of use of his own funds that occurred as a result of the Data Breach.

77. Plaintiff would not have used his credit card to make purchases from the ShopRuger.com website had Ruger disclosed that it lacked adequate computer systems and data

security practices to safeguard customers' personal and financial information from theft, and that it was subject to an ongoing data breach at the time Plaintiff made his purchase. Ruger also failed to provide Plaintiff with timely and accurate notice of the data breach, instead noticing him seven months later.

78. Plaintiff suffered actual injury from having his Private Information compromised and/or stolen as a result of the Data Breach.

79. Plaintiff suffered actual injury and damages in paying money to and ordering products from Ruger during the Data Breach that he would not have paid or ordered had Ruger disclosed that it lacked computer systems and data security practices adequate to safeguard customers' personal and financial information and had Ruger provided timely and accurate notice of the Data Breach.

80. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his personal and financial information – a form of intangible property that the Plaintiff entrusted to Ruger for the purpose of making purchases on its website and which was compromised in, and as a result of, the Data Breach.

81. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by his personal and financial information being placed in the hands of criminals who have already misused such information stolen in the Data Breach.

82. Plaintiff has a continuing interest in ensuring that his Private Information, which remains in the possession of Ruger, is protected and safeguarded from future breaches.

83. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing

credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by Defendant. Plaintiff has spent several hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

84. As a result of the Data Breach, Plaintiff has suffered anxiety as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity crimes, fraud, and theft. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

85. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant obtained from Plaintiff; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

86. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

CLASS ACTION ALLEGATIONS

87. Plaintiff brings this nationwide class action on behalf of himself and all others similarly situated under Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

88. The Class that Plaintiff seeks to represent is defined as follows:

> **All persons Defendant identified as being among those individuals impacted by the Data Breach, including all persons who were sent a notice of the Data Breach.**

89. Excluded from the Class are Defendant's officers and directors; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families, and Members of their staff.

90. Plaintiff reserves the right to amend or modify the Class definition and/or create additional subclasses as this case progresses.

91. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of at least 167,936[24] current and former customers of Defendant whose sensitive data was compromised in Data Breach.

92. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

[24] See *Data Breach Notifications*, OFF. ME. ATT'Y GEN., https://apps.web.maine.gov/online/aeviewer/ME/40/d7e85c2c-cf60-4b20-8d04-537dcd5b2504.shtml (last visited September 25, 2022).

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their PII and PCD;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

l. Whether Defendant breach implied or express contracts with Plaintiff and Class Members;

m. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

n. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

o. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

93. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

94. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class and has no interests antagonistic to those of other Class Members. Plaintiff's counsel are competent and experienced in litigating Class actions.

95. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

96. 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 likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management

difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

97. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

COUNT I
Negligence
(on behalf of Plaintiff and Class Members)

98. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

99. Ruger solicited and gathered the Private Information, including the PCD, of Plaintiff and Class Members to facilitate sales transactions.

100. Ruger knew, or should have known, of the risks inherent in collecting the PII and PCD of Plaintiff and the Class Members and the importance of adequate security. Ruger also knew about numerous, well-publicized payment card data breaches involving other national retailers.

101. Ruger owed duties of care to Plaintiff and the Class Members whose Private Information was entrusted to it. Ruger's duties included the following:

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

b. To exercise reasonable care in selecting its third-party vendors and monitoring and auditing their data security practices to ensure compliance with legal and industry standards and obligations;

c. To protect customers' Private Information using reasonable and adequate security procedures and systems that are compliant with the PCI DSS and consistent with industry-standard practices;

d. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

e. To promptly notify Plaintiff and Class Members of the data breach.

102. By collecting this data, and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property, to prevent disclosure of the Private Information, and to safeguard the Private Information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

103. Ruger's duty of care extended to ensuring that any third-party vendors it hired and that had exposure to the Private Information of Plaintiff and Class Members would implement adequate measures to prevent and detect cyber intrusions.

104. Because Ruger knew that a breach of its systems would damage thousands of its customers, including Plaintiff and Class Members, it had a duty to adequately protect their Private Information.

105. Ruger owed a duty of care not to subject Plaintiff and the Class Members to an unreasonable risk of harm because they were the foreseeable and probable victims of any inadequate security practices.

106. Ruger had a duty to implement, maintain, and ensure reasonable security procedures and practices to safeguard Plaintiff's and Class Members' Private Information.

107. Ruger knew, or should have known, that its computer systems and security practices did not adequately safeguard the Private Information of Plaintiff and the Class Members.

108. Ruger knew, or should have known, that the computer systems and security practices of its third-party vendors did not adequately safeguard the Private Information of Plaintiff and the Class Members.

109. Ruger breached its duties of care by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and the Class Members.

110. Ruger breached its duties of care by failing to provide prompt notice of the data breach to the persons whose PII and PCD was compromised.

111. Ruger acted with reckless disregard for the security of the Private Information of Plaintiff and the Class Members because Ruger knew or should have known that its computer systems and data security practices, and those of its third-party vendors, were not adequate to safeguard the PII and PCD that that it collected, which hackers targeted in the Data Breach.

112. Ruger acted with reckless disregard for the rights of Plaintiff and the Class Members by failing to provide prompt and adequate notice of the data breach so that they could take measures to protect themselves from damages caused by the fraudulent use the Private Information compromised in the data breach.

113. Ruger had a special relationship with Plaintiff and the Class Members. Plaintiff's and the Class Members' willingness to entrust Ruger with their Private Information was predicated on the mutual understanding that Ruger would implement adequate security precautions. Moreover, Ruger was in an exclusive position to protect its systems (and the Private Information) from attack. Plaintiff and Class Members relied on Ruger to protect their Private Information.

114. Ruger's own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their PII and PCD. Ruger's misconduct included failing to:

a. Secure its e-commerce website;

b. Secure access to its and its vendors' servers;

c. Audit and monitor its vendors;

d. Comply with industry standard security practices;

e. Follow the PCI-DSS standards;

f. Encrypt PCD at the point-of-sale and during transit;

g. Employ adequate network segmentation;

h. Implement adequate system and event monitoring;

i. Utilize modern payment systems that provided more security against intrusion;

j. Install updates and patches in a timely manner; and

k. Implement the systems, policies, and procedures necessary to prevent this type of data breach.

115. Ruger also had independent duties under the FTC Act and state laws that required it to reasonably safeguard Plaintiff's and the Class Members' PII and PCD and promptly notify them about the data breach.

116. Ruger breached the duties it owed to Plaintiff and Class Members in numerous ways, including:

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

b. By failing to implement adequate security systems, protocols and practices sufficient to protect their PII and PCD both before and after learning of the Data Breach;

c. By failing to comply with the minimum industry data security standards, including the PCI-DSS, during the period of the Data Breach, and

d. By failing to timely and accurately disclose that the PII and PCD of Plaintiff and the Class had been improperly acquired or accessed.

117. But for Ruger's wrongful and negligent breach of the duties it owed Plaintiff and the Class Members, their personal and financial information either would not have been compromised or they would have been able to prevent some or all of their damages.

118. As a direct and proximate result of Ruger's negligent conduct, Plaintiff and the Class Members have suffered damages and are at imminent risk of further harm.

119. The injury and harm that Plaintiff and Class Members suffered (as alleged above) was reasonably foreseeable.

120. The injury and harm that Plaintiff and Class Members suffered (as alleged above) was the direct and proximate result of Ruger's negligent conduct.

121. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
Breach of Implied Contract
(on behalf of Plaintiff and Class Members)

122. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

123. When Plaintiff and Class Members provided their PII and PCD to Ruger in making purchases on its website, they entered into implied contracts under which Ruger agreed to protect their PII and PCD and timely notify them in the event of a data breach.

124. Ruger invited its customers, including Plaintiff and the Class, to make purchases on its website using payment cards in order to increase sales by making purchases more convenient.

125. An implicit part of the offer was that Ruger would safeguard their Private Information using reasonable or industry-standard means and would timely notify Plaintiff and the Class in the event of a data breach.

126. Ruger also affirmatively represented in its Privacy Policy that it protected the Private Information of Plaintiff and the Class in several ways, as described above.

127. Based on the implicit understanding and also on Ruger's representations, Plaintiff and the Class accepted the offers and provided Ruger with their PII and PCD by using their payment cards in connection with purchases on the Ruger website during the period of the data breach.

128. Ruger manifested its intent to enter into an implied contract that included a contractual obligation to reasonably protect Plaintiff's and Class Members' PII and PCD through, among other things, its Privacy Notice.

129. Ruger further demonstrated an intent to safeguard the Private Information of Plaintiff and Class Members through its conduct. No reasonable person would provide sensitive, non-public information to a retailer without the implicit understanding that the retailer would maintain that information as confidential.

130. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

131. Plaintiff and Class Members would not have provided their PII and PCD to Ruger had they known that Ruger would not safeguard their PII and PCD as promised or provide timely notice of a data breach.

132. Plaintiff and Class Members fully performed their obligations under the implied contracts with Ruger.

133. Ruger breached the implied contracts by failing to safeguard Plaintiff's and Class Members' Private Information and failing to provide them with timely and accurate notice when their Private Information was compromised in the Data Breach.

134. The losses and damages Plaintiff and Class Members sustained (as described above) were the direct and proximate result of Ruger's breaches of its implied contracts with them.

COUNT III
Unjust Enrichment
(on behalf of Plaintiff and Class Members)

135. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

136. This claim is brought in the alternative to Plaintiff's claim for breach of implied contract.

137. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by Plaintiff and Class Members.

138. As such, a portion of the payments made by Plaintiff and Class Members was to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

139. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and in so doing provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

140. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

141. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information and instead directing those funds to its own profit. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

142. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

143. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

144. Plaintiff and the Class have no adequate remedy at law.

145. Under the circumstances, it would be unjust for Ruger to be permitted to retain any of the benefits that Plaintiff and Class Members of the Class conferred on it.

146. Ruger should be compelled to disgorge into a common fund or constructive trust for the benefit of Plaintiff and Class Members proceeds that it unjustly received from them. In the alternative, Ruger should be compelled to refund the amounts that Plaintiff and the Class overpaid, plus attorneys' fees, costs, and interest thereon.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and his counsel as Class Counsel;

B. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the classes as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Classes requested herein;

C. Judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, attorney's fees, statutory costs, and such other and further relief as is just and proper;

D. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

E. An order requiring Ruger to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

F. A judgment in favor of Plaintiff and the Classes awarding them pre-judgment and post judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

G. An award of such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

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

Dated: October 4, 2022

SCOTT+SCOTT ATTORNEYS AT LAW LLP

/s/ Joseph P. Guglielmo
Joseph P. Guglielmo (CT 27481)
The Helmsley Building
230 Park Avenue,17th Floor
New York, NY 10169
Tel.: 212-23-6444
Fax: 212-223-6334
jguglielmo@scott-scott.com

Anja Rusi (CT 30686)
SCOTT+SCOTT ATTORNEYS AT LAW LLP
156 South Main Street
P.O. Box 192
Colchester, CT 06415
Tel.: 860-537-5537
Fax: 860-537-4432
arusi@scott-scott.com

Terence R. Coates (*pro hac vice* forthcoming)
Justin C. Walker (*pro hac vice* forthcoming)
Dylan J. Gould (*pro hac vice* forthcoming)
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Tel.: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
jwalker@msdlegal.com
dgould@msdlegal.com

Gary M. Klinger (*pro hac vice* forthcoming)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
221 West Monroe Street, Suite 2100

Chicago, IL 60606
Tel.: (847) 208-4585
gklinger@milberg.com

Attorneys for Plaintiff and the Proposed Class