UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF CONNECTICUT

MARK JONES, MICHELLE GOULD, DICKY WARREN, CARL JUNG, LAUREN COPELAND and LEE WOODS, *individually and on behalf of all others similarly situated*, **Plaintiffs,** **v.** **STURM, RUGER & COMPANY, INC. and FREESTYLE SOFTWARE, INC.,** **Defendants.**	**Civil Action No.: 3:2022cv01233** **FIRST AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED** **Date: January 19, 2023**

Plaintiffs Mark Jones, Michelle Gould, Dicky Warren, Carl Jung, Lauren Copeland and Lee Woods ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this First Amended Class Action Complaint ("Complaint") against Defendants Sturm, Ruger & Company, Inc. ("Ruger") and Freestyle Software, Inc. ("Freestyle" and collectively with Ruger "Defendants"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendants. Plaintiffs make the following allegations upon information and belief, except as to their own actions, which are made on personal knowledge, the investigation of their 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, and Freestyle Software, Inc. d/b/a Freestyle Solutions, a software developer for order processing, inventory tracking and purchase fulfillment for eCommerce platforms, with its principal place of business in Parsippany, New Jersey.

2. Ruger owns the website www.ShopRuger.com ("ShopRuger.com") where it sells certain products and merchandise directly to consumers. Freestyle hosted and provided software and/or services for the ShopRuger.com website. To make a purchase or register an account on ShopRuger.com, Plaintiffs and the Class Members were required to provide certain sensitive, non-public information to Defendants. Unfortunately, Defendants 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 Plaintiffs and the Class Members in order for criminals to use that information in furtherance of theft, identity crimes, and fraud.

4. Defendants' failure to prevent and detect the Data Breach is particularly egregious considering the nature of Ruger's business and the Private Information they collected. The aggregate information acquired by cybercriminals in this Data Breach is particularly concerning considering that Defendants' customers were purchasing firearm accessories from ShopRuger.com. Criminals can now access Plaintiffs' and the Class Members' 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. Plaintiffs bring this class action against Defendants to seek damages for themselves 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 Plaintiffs 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 Plaintiffs and Class Members, that Freestyle, its third-party vendor (and agent), 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 server that housed the ShopRuger.com website, allowing the Private Information of Plaintiffs and Class Members to be captured and compromised by data thieves.[1]

7. As a result of Defendants' failure to prevent the Data Breach, or detect it during the nearly one-and-a-half years that criminals were siphoning Ruger's 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 Defendants' conduct, which includes: (a) refusing to take adequate and reasonable measures to ensure their data systems were protected; (b) refusing to take available steps to prevent the breach from happening; (c) Ruger failing to adequately audit and monitor its third party data security vendor Freestyle; (d) Ruger failing to disclose to their customers the material fact that Defendants 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 Plaintiffs and Class Members as a direct result of the Data

[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/ (last visited Jan. 16, 2023).

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 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. An increased risk of being targeted for burglary because criminals now have an up-to-date list of gun owners, along with home addresses, and guns are

very attractive targets for criminals given their inherent value and their ability to be used in other criminal activity;

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

i. Money paid to Ruger during the period of the Data Breach in that Plaintiffs and Class Members would not have purchased from Ruger, or would have paid less for their purchases, had Defendants disclosed that they lacked adequate systems and procedures to reasonably safeguard customers' Private Information and had Plaintiffs and Class Members known that Defendants would not provide timely and accurate notice of the Data Breach; and

j. Continued risk to their PII and PCD, which remains in the possession of Ruger and Freestyle, and which is subject to further breaches so long as Defendants continue to fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data in their possession.

9. Examples of the harms to Defendants' customers as a direct and foreseeable consequence of their conduct include the experiences of the representative Plaintiffs, which are described below.

THE PARTIES

Plaintiffs

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

11. Plaintiff Michelle Gould is, and was, a citizen of the State of Arizona residing in the City of Peoria.

12. Plaintiff Dicky Warren is, and was, a citizen of the State of Tennessee residing in the City of Henry.

13. Plaintiff Carl Jung is, and was, a citizen of the State of Missouri residing in the City of Wildwood.

14. Plaintiff Lee Woods, is, and was, a citizen of the State of Texas residing in the City of San Antonio.

15. Plaintiff Lauren Copeland is, and was, a citizen of the State of Michigan residing in the City of Harper Woods.

Defendants

16. Sturm, Ruger & Company, Inc. is, and was, a publicly traded corporation incorporated in the State of Delaware. Ruger's headquarters is located at 1 Lacey Place, Southport, Connecticut 06890.

17. Defendant Freestyle Software, Inc., a Delaware corporation with its principal place of business in the State of New Jersey, is, and was, a software company that provides website hosting and eCommerce solutions to online businesses seeking to sell goods and services directly to consumers.

JURISDICTION & VENUE

18. 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 Defendants to establish minimal diversity.

19. The District of Connecticut has personal jurisdiction over Defendants because Ruger and/or its parents or affiliates are headquartered in this District and Ruger and Freestyle both conduct substantial business in Connecticut and in this District. In addition, both Defendants have consented to jurisdiction in this District.

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

FACTUAL ALLEGATIONS

Background

21. 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]

22. 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,

[2] Sturm Ruger & Co. Inc., Annual Report, (Form 10-K) (Feb. 23, 2022), https://sec.report/Document/0001174947-22-000269/ (last visited Jan. 16, 2023).

pepper spray, cleaning supplies, shooting supplies, safety equipment, survival gear, hunting gear, as well as other types of sporting accessories and apparel, directly to retail purchasers.[3]

23. Freestyle is a software company that works in the eCommerce sector. The software that Freestyle provides allows eCommerce websites to sell goods and services to consumers, like Plaintiffs and Class Members.[4] Freestyle's business would not be possible without the collection and aggregation of consumer data for eCommerce storefronts, like the website at issue in this case (ShopRuger.com) on which it relies to process transactions. In the course of this business, Freestyle collects, at a minimum, the PII and PCD that were compromised in the Data Breach as alleged herein.

24. Ruger contracts with Freestyle to provide inventory and order management services for its website ShopRuger.com. 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, credit or debit card number, and Citizenship Information (for some items such as magazines, barrels, and similar parts).[5]

25. 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 Ruger's newsletter and promotions, provide certain other services, and so that it may otherwise continue to correspond with customers.[6]

26. When they provided their Private Information to Defendants, Plaintiffs and Class Members relied on Defendants (both sophisticated companies, knowledgeable in the area of

---

3 *See* Sturm Ruger & Co. Inc., https://shopruger.com (last visited Jan. 16, 2023).

4 https://www.freestylesolutions.com/our-software (last visited Jan. 16, 2023).

5 *Privacy Policy*, https://shopruger.com/privacy.asp (last visited Jan. 16, 2023).

6 *Id.*

internet retailing) to keep Plaintiffs' and Class Members' Private Information confidential and securely maintained, to use this information for business purposes only, and to only make authorized disclosures of this information.

27. Defendants had a duty to take reasonable measures to protect the Private Information of Plaintiffs 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.

28. Defendants also recognized and voluntarily adopted additional duties to protect PII and PCD in the Ruger Privacy Policy ("Privacy Policy"), which has been publicly posted to the internet.[7] In its Privacy Policy, Ruger 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."[8]

29. Freestyle, as a sophisticated software and website hosting provider, also understands the importance of maintaining PII and PCD as private and confidential. Freestyle's own terms of use prohibit both "violating the privacy rights of others," and "the collection of information about individuals without their knowledge or consent."[9] Despite this, Freestyle failed to implement adequate data security measures, to prevent or detect the Data Breach, and to timely and adequately notify Plaintiffs and Class Members that their most sensitive information had been stolen by criminals.

---

7 *Id.*

8 *Id.*

9 https://www.freestylesolutions.com/company/terms-and-conditions/ (last visited Jan. 16, 2023).

30. Despite these duties and promises, Defendants allowed data thieves to infect and infiltrate the ShopRuger.com website and steal the Private Information of thousands of Ruger's customers. According to data that Ruger disclosed to the Maine Attorney General, the breach affected 167,963 Ruger customers.[10]

The Data Breach Was Foreseeable

31. Defendants had obligations created by statute, industry standards, and common law to Plaintiffs and Class Members to keep Plaintiffs' and Class Members' PII and PCD confidential and to protect their PII and PCD from unauthorized access and disclosure.

32. Plaintiffs and Class Members provided their PII and PCD to Defendants with the reasonable expectation and the mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

33. Defendants' data security obligations were particularly important given the substantial increase in malware attacks and/or data breaches of industry leaders preceding the date of the breach.

34. Data breaches have become extremely widespread. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.

35. 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), Defendants knew or should have known that the Private Information that they

[10] https://apps.web.maine.gov/online/aeviewer/ME/40/d7e85c2c-cf60-4b20-8d04-537dcd5b2504.shtml (last visited Jan. 16, 2023).

collected and maintained would be targeted by cybercriminals.

36. 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.

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

The Data Breach

38. In the Notice Letter, dated August 18, 2022, Ruger notified various state Attorneys General, as well as Plaintiffs and Class Members, that its third-party software vendor, Freestyle, that owns and manages the server hosting ShopRuger.com, experienced a data breach where the Private Information of certain Ruger customers was "captured and potentially accessed by an unauthorized party."[11]

39. The Notice Letter informed Plaintiffs 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."[12]

40. The Private Information exfiltrated in the Data Breach was unencrypted and captured directly from the checkout page at ShopRuger.com.[13]

41. Incredibly, the malicious malware infected ShopRuger.com for a period of nearly

---

11 *Supra*, note 1.

12 *Id*.

13 *Id*.

17 months, from September 18, 2020 through February 3, 2022.[14]

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

43. Despite Ruger'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 Defendant Ruger 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 . . . ."[15] Freestyle also failed to implement adequate regular security reviews or audits of its website, servers, and networks, and Ruger negligently failed to ensure such reviews or audits were performed, which would have alerted Defendants to the presence of malware sooner than the approximately 17 months it remained undetected.

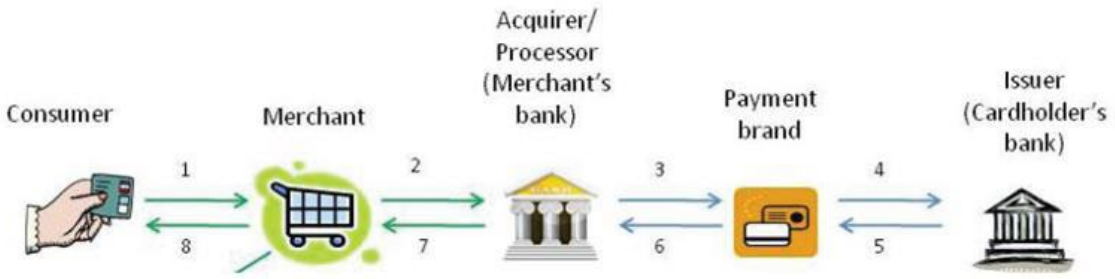
Securing PII and PCD and Preventing Breaches

44. 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

14 *Id.*

15 *Supra*, note 1.

(*i.e.*, the cardholder's bank). The issuer then notifies the payment card company of its decision to authorize or reject the transaction. See graphic below:[16]



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.

45. 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.

46. Encryption mitigates security weaknesses that exist when cardholder data has been

[16] *Payments 101: Credit and Debit Card Payments*, FIRST DATA, at 7 (Oct. 2010), http://euro.ecom.cmu.edu/resources/elibrary/epay/Payments-101.pdf (last visited Jan. 16, 2023).

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.

Defendants Failed to Follow FTC Guidelines

47. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

48. According to the FTC, the need for data security should be factored into all business decision-making.

49. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.

50. The guidelines note that businesses should protect the personal information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems.

51. 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.

52. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for

suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

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

54. Defendants failed to properly implement basic data security practices.

55. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII and PCD constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

56. Defendants were at all times fully aware of their obligation to protect the PII and PCD of the customers for whom they stored PII and PCD. Defendants were also aware of the significant repercussions that would result from their failure to do so.

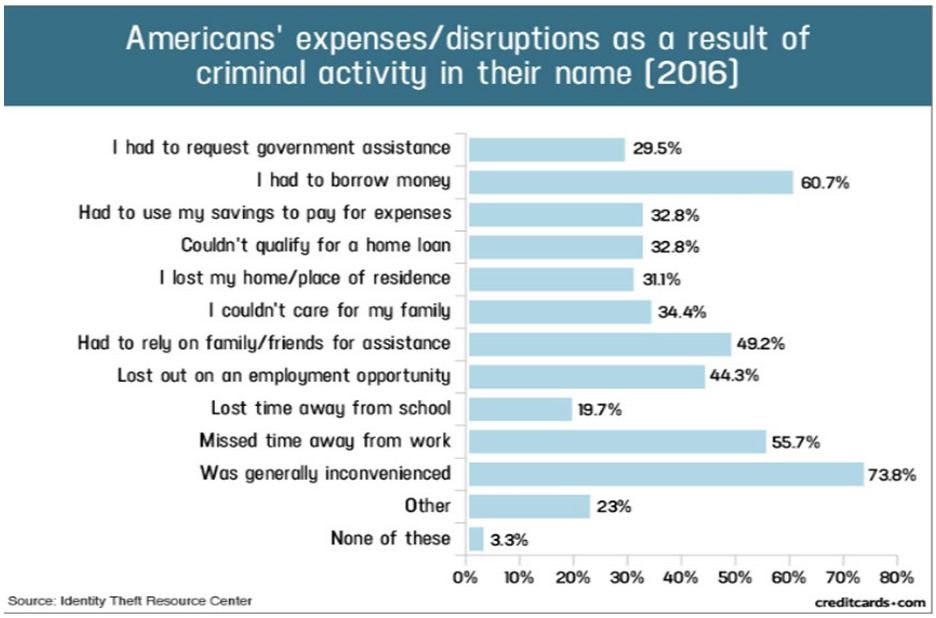
The Harm Consumers Will Face Because of Defendants' Data Breach

57. The financial fraud suffered by Plaintiffs and Class Members demonstrates that Ruger and Freestyle chose not to invest in the technology to encrypt 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.

58. 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.

59. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of Private Information:[17]



60. Plaintiffs and Class Members have experienced one or more of these harms as a result of the Data Breach.

61. 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.

62. Moreover, there may be a time lag between when harm occurs versus when it is

[17] 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 Jan. 16, 2023).

discovered, and also between when PII and PCD are stolen and when they are 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.[18]

63. PII 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.

64. 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 Plaintiffs and Class Members are at an increased risk of fraud for many years into the future. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts for many years to come.

65. Plaintiffs 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;

---

[18] 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 (last visited January 16, 2023).

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.

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

67. Plaintiffs' Private Information was compromised as a direct and proximate result of the Data Breach.

68. As a direct and proximate result of the Data Breach, Plaintiffs' PII and PCD were "skimmed" and exfiltrated and are in the hands of identity thieves and criminals, as evidenced by the fraud perpetrated against Plaintiffs described above and further below.

69. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered actual fraud.

70. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud. Plaintiffs 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.

71. Plaintiffs 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.

72. Plaintiffs and Class Members also suffered a loss of value of their PII and PCD when they were acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

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

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

75. Plaintiffs 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 impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

d. Damages flowing from Defendants' 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 their 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 they were permitted to obtain from their accounts.

76. The substantial delay in providing notice of the Data Breach deprived Plaintiffs and the Class Members of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach. As a result of Defendants' delay in notifying consumers of the Data Breach, the risk of fraud for Plaintiffs and Class Members was and has been driven even higher.

77. The Private Information 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.[19] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[20] Criminals can

[19] 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/ (last visited Jan. 16, 2023).

[20] 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/ (last visited Jan. 16, 2023).

also purchase access to entire company data breaches from $900 to $4,500.

78. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[21] 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.[22, 23] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[24]

79. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished due to its acquisition by cybercriminals. This transfer of value occurred without any consideration paid to Plaintiffs 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.

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

81. 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.

---

[21] 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 (last visited Jan. 16, 2023).

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

[23] *What is digi.me?*, *DIGI.ME,* https://digi.me/what-is-digime/ (last visited Jan. 16, 2023).

[24] *Frequently Asked Questions*, Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Jan. 16, 2023).

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.[25]

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

83. Plaintiffs 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.

84. In addition to the traditional financial harms that are common to data breaches of this type, Ruger is a firearms manufacturer and this data breach included information regarding the nature of each purchase. This means that the cyber criminals now have a ready, up-to-date list of homes with firearms. Guns represent a particularly attractive target for criminals, given both their value and their use in other criminal enterprises. According to a 2017 study published in the journal "Injury Epidemiology," approximately 380,000 guns are stolen every year in this country.[26] That represents a more than 60% increase from a 2012 Department of Justice survey

---

[25] *Supra*, note 18.

[26] Hemenway, D., et al. *Whose guns are stolen? The epidemiology of Gun theft victims* (Inj. Epidemiol., Dec. 2017), *available at* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5385318/ (last visited Jan. 16, 2023).

that found that between 2005 and 2010 on average 232,400 guns were stolen each year.[27] Given the rising prevalence of gun theft, the fact that criminals now know that Plaintiffs and Class Members own guns and have a recent address for where their guns are kept means that Plaintiffs and Class Members must take extra precautions to safeguard themselves and their firearms for years to come and must live in fear that they will be targeted for theft simply for making a purchase on the ShopRuger.com website.

85. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' 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.

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

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

[27] Langton, L., *Firearms Stolen during Household Burglaries and Other Property Crimes, 2005–2010* (Bureau of Justice Statistics, Nov. 2012), *available at* https://bjs.ojp.gov/content/pub/pdf/fshbopc0510.pdf (last visited Jan. 16, 2023).

PLAINTIFFS' EXPERIENCES

Plaintiff Mark Jones

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

89. The ShopRuger.com website was hosted on Defendant Freestyle's servers.

90. After his transaction on Defendants' website, Plaintiff Jones experienced five fraudulent purchases on his Discover credit card.

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

92. Plaintiff Jones received a Notice Letter from Ruger dated August 18, 2022, informing him that Freestyle had sustained a data breach and that Plaintiff Jones' PII and PCD were captured and compromised. This letter was sent seven months after Defendant Freestyle learned about the Data Breach.

93. The Notice Letter from Ruger informed Plaintiff Jones that unauthorized individuals may have gained access to his PII and PCD when he completed his transactions on ShopRuger.com.

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

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

96. Plaintiff Jones 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.

97. Plaintiff Jones was not reimbursed for the loss of use of, loss of access to, or restrictions placed upon his account that occurred as a result of the Data Breach.

98. Plaintiff Jones would not have used his Discover credit card to make purchases from the ShopRuger.com website had Defendants timely disclosed that the website lacked adequate computer systems and data security practices to safeguard customers' personal and financial information from theft, and that the website was subject to an ongoing data breach at the time Plaintiff Jones made his purchase. Defendants also failed to provide Plaintiff Jones with timely and accurate notice of the Data Breach, instead noticing him seven months after they learned about the Data Breach.

99. Plaintiff Jones suffered actual injury from having his PII and PCD compromised and/or stolen as a result of the Data Breach.

100. Plaintiff Jones 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 Defendants disclosed that the ShopRuger.com website lacked computer systems and data security practices adequate to safeguard customers' personal and financial information and had Defendants provided timely and accurate notice of the Data Breach.

101. Plaintiff Jones 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 Plaintiff Jones entrusted to Defendants for the purpose of making purchases on the ShopRuger.com website and which was compromised in, and as a result of, the Data Breach.

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

103. Plaintiff Jones has a continuing interest in ensuring that his PII and PCD, which remain in the possession of Defendants, are protected and safeguarded from future breaches.

104. As a result of the Data Breach, Plaintiff Jones 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 Defendants. Plaintiff Jones has spent several hours dealing with the Data Breach, valuable time Plaintiff Jones otherwise would have spent on other activities.

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

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

107. As a result of the Data Breach, Plaintiff Jones 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 Jones is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Michelle Gould

108. During the relevant period, Plaintiff Gould made a purchase from the ShopRuger.com website, which was hosted on Defendant Freestyle's servers.

109. Plaintiff Gould visited Ruger's website and provided Ruger with her PII and PCD by using her debit card to make purchases on ShopRuger.com.

110. Subsequent to making the purchase from ShopRuger.com, Plaintiff Gould received a letter dated August 18, 2022 from Ruger informing Plaintiff Gould that she was the victim of the Data Breach. However, this letter was sent seven months after Defendant Freestyle learned about the Data Breach.

111. The Notice Letter from Ruger informed Plaintiff Gould that Freestyle had sustained a data breach and that Plaintiff Gould's PII and PCD were captured and compromised as a result of the Data Breach.

112. The Notice Letter indicated that the ShopRuger.com website was hosted on Defendant Freestyle's servers.

113. After her transaction on Defendant Ruger's website, on or around September 18, 2022, Plaintiff Gould experienced multiple, rapid succession, fraudulent transactions on her bank account where cyber criminals stole more than $1,300 from her. The bank account was connected with the debit card used to make purchases on ShopRuger.com.

114. As a result of the fraudulent charges on Plaintiff Gould's debit card, she was forced to spend time corresponding with her card issuer to address the fraudulent charges. During this extended period of time, Plaintiff Gould had limited access to her funds.

115. In addition, Plaintiff Gould has been informed by her credit monitoring service that her primary email address was found on the Dark Web.

116. Plaintiff Gould suffered actual injury in the form of time spent dealing with fraud and the increased risk of fraud resulting from the Data Breach and/or monitoring her accounts for fraud.

117. Plaintiff Gould suffered actual injury in the form of fraudulent charges on her debit card and the loss of use of her funds while disputing the unauthorized charge and additional damages resulting from such loss of use.

118. Plaintiff Gould was not reimbursed for the loss of use of, loss of access to, or restrictions placed upon her account that occurred as a result of the Data Breach.

119. Plaintiff Gould would not have used her debit card to make purchases from the ShopRuger.com website had Defendants timely disclosed that the website lacked adequate computer systems and data security practices to safeguard customers' personal and financial information from theft, and that the website was subject to an ongoing data breach at the time Plaintiff Gould made her purchase. Defendants also failed to provide Plaintiff Gould with timely and accurate notice of the Data Breach, instead noticing her seven months after Defendants learned about the Data Breach.

120. Plaintiff Gould suffered actual injury from having her PII and PCD compromised and/or stolen as a result of the Data Breach.

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

122. Plaintiff Gould suffered actual injury in the form of damages to and diminution in the value of her PII and PCD – a form of intangible property that Plaintiff Gould entrusted to Defendants for the purpose of making purchases on the ShopRuger.com website and which was compromised in, and as a result of, the Data Breach.

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

124. Plaintiff Gould made reasonable efforts to mitigate the impact of the Data Breach after receiving the Notice letter.

125. Plaintiff Gould has a continuing interest in ensuring that her PII and PCD, which remain in the possession of Defendants, are protected and safeguarded from future breaches.

126. As a result of the Data Breach, Plaintiff Gould 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 and enrolling in credit monitoring and identity theft protection services offered by Defendants. Plaintiff Gould has spent several hours dealing with the Data Breach, valuable time Plaintiff Gould otherwise would have spent on other activities.

127. Plaintiff Gould has paid out of pocket costs by paying a monthly fee for credit and identity protection services through AAA.

128. As a result of the Data Breach, Plaintiff Gould has suffered anxiety as a result of her PII and PCD being compromised, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII and PCD for purposes of identity crimes, fraud, burglary, and theft. Plaintiff Gould is very concerned about identity theft, burglary, and fraud, as well as the consequences of such identity theft, burglary, and fraud resulting from the Data Breach.

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

130. As a result of the Data Breach, Plaintiff Gould 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 Gould is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Dicky Warren

131. During the relevant period, Plaintiff Warren made a purchase from the ShopRuger.com website, which was hosted on Defendant Freestyle's servers.

132. Plaintiff Warren used one of his debit/credit cards to make this purchase.

133. Subsequent to making this purchase, Plaintiff Warren received a letter dated August 18, 2022 from Ruger informing Plaintiff Warren that he was the victim of the Data Breach.

However, this letter was sent seven months after Defendant Freestyle learned about the Data Breach.

134. The Notice Letter informed Plaintiff Warren that malware was placed on Defendant Freestyle's servers and that the malware, installed by cybercriminals, allowed those cybercriminals to gain access to his PII and PCD which he used to make his purchase through Defendant Freestyle's servers.

135. Plaintiff Warren's PII and PCD were compromised in the Data Breach and were likely stolen and in the hands of cybercriminals who illegally accessed Defendants' network for the specific purpose of targeting the PII and PCD.

136. Plaintiff Warren typically takes measures to protect his PII and PCD and is very careful about sharing his PII and PCD.

137. Plaintiff Warren stores any documents containing his PII and PCD in a safe and secure location and he diligently chooses unique usernames and passwords for his online accounts.

138. As a result of the Data Breach, Plaintiff Warren has spent and continues to spend a considerable amount of time on issues related to this Data Breach. This is time that was lost and unproductive and took away from other activities and duties.

139. As a result of the Data Breach, Plaintiff Warren made reasonable efforts to mitigate the impact of the Data Breach after receiving the Notice Letter.

140. Plaintiff Warren also suffered actual injury in the form of damages to and diminution in the value of his PII and PCD— a form of intangible property that he entrusted to Defendants for the purpose of processing transactions, which was compromised in and as a result of the Data Breach.

141. Plaintiff Warren suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

142. Plaintiff Warren has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PCD, particularly his sensitive purchases in combination with his home address, being placed in the hands of criminals.

143. Defendants obtained and continue to maintain Plaintiff Warren's PII and PCD and have a continuing legal duty and obligation to protect that PII and PCD from unauthorized access and disclosure. Defendants required the PII and PCD from Plaintiff Warren when he made purchases from Ruger's website. Plaintiff Warren, however, would not have entrusted his PII and PCD to Defendants had he known that they would fail to maintain adequate data security. Plaintiff Warren's PII and PCD were compromised and disclosed as a result of the Data Breach.

144. As a result of the Data Breach, Plaintiff Warren 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 Warren is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Carl Jung

145. During the relevant period, Plaintiff Jung made a purchase from the ShopRuger.com website, which was hosted on Defendant Freestyle's servers.

146. Plaintiff Jung used one of his debit/credit cards to make this purchase.

147. Subsequent to making this purchase, Plaintiff Jung received a letter dated August 18, 2022 from Ruger informing Plaintiff Jung that he was the victim of Defendants' Data Breach.

However, this letter was sent seven months after Defendant Freestyle learned about the Data Breach.

148. The Notice Letter informed Plaintiff Jung that malware was placed on Defendant Freestyle's servers and that the malware, installed by cybercriminals, allowed those cybercriminals to gain access to his PII and PCD which he used to make his purchase through Defendant Freestyle's servers.

149. Plaintiff Jung's PII and PCD were compromised in the Data Breach and were likely stolen and in the hands of cybercriminals who illegally accessed Defendants' network for the specific purpose of targeting the PII and PCD.

150. Plaintiff Jung typically takes measures to protect his PII and PCD and is very careful about sharing his PII and PCD.

151. Plaintiff Jung stores any documents containing his PII and PCD in a safe and secure location and he diligently chooses unique usernames and passwords for his online accounts.

152. As a result of the Data Breach, Plaintiff Jung has spent and continues to spend a considerable amount of time on issues related to this Data Breach. This is time that was lost and unproductive and took away from other activities and duties.

153. As a result of the Data Breach, Plaintiff Jung made reasonable efforts to mitigate the impact of the Data Breach after receiving the Notice Letter.

154. Plaintiff Jung also suffered actual injury in the form of damages to and diminution in the value of his PII and PCD — a form of intangible property that he entrusted to Defendants for the purpose of processing transactions, which was compromised in and as a result of the Data Breach.

155. Plaintiff Jung suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

156. Plaintiff Jung has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PCD, particularly his sensitive purchases in combination with his home address, being placed in the hands of criminals.

157. Defendants obtained and continue to maintain Plaintiff Jung's PII and PCD and have a continuing legal duty and obligation to protect that PII and PCD from unauthorized access and disclosure. Defendants required the PII and PCD from Plaintiff Jung when he made purchases from Ruger's website. Plaintiff Jung, however, would not have entrusted his PII and PCD to Defendants had he known that they would fail to maintain adequate data security. Plaintiff Jung's PII and PCD were compromised and disclosed as a result of the Data Breach.

158. As a result of the Data Breach, Plaintiff Jung 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 Jung is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Lauren Copeland

159. During the relevant period, Plaintiff Copeland made a purchase from the ShopRuger.com website, which was hosted on Defendant Freestyle's servers.

160. Plaintiff Copeland used one of her debit/credit cards to make this purchase.

161. Subsequent to making this purchase, Plaintiff Copeland received a letter dated August 18, 2022 from Ruger informing Plaintiff Copeland that she was the victim of Defendants'

Data Breach. However, this letter was sent seven months after Defendant Freestyle learned about the Data Breach.

162. The Notice Letter from Ruger informed Plaintiff Copeland that Defendant Freestyle had sustained a data breach and that Plaintiff Copeland's PII and PCD were captured and compromised as a result of the Data Breach.

163. The Notice Letter indicated that the ShopRuger.com website was hosted on Defendant Freestyle's servers.

164. Plaintiff Copeland's PII and PCD were likely stolen and are in the hands of cybercriminals who illegally accessed Defendants' network for the specific purpose of targeting the PII and PCD.

165. During the relevant time period, Plaintiff Copeland found multiple unauthorized transactions on her bank account. Plaintiff Copeland spent time reporting these unauthorized transactions to her bank and working with the bank to investigate the unauthorized transactions.

166. In addition, Plaintiff Copeland's bank has twice had to cancel her debit card and issue her new debit cards. As a result, Plaintiff Copeland spent time dealing with her cards' reissuance.

167. Plaintiff Copeland typically takes measures to protect her PII and PCD and is very careful about sharing her PII and PCD.

168. As a result of the Data Breach, Plaintiff Copeland has spent and continues to spend a considerable amount of time on issues related to this Data Breach. This is time that was lost and unproductive and took away from other activities and duties.

169. As a result of the Data Breach, Plaintiff Copeland made reasonable efforts to mitigate the impact of the Data Breach after receiving the Notice Letter.

170. Plaintiff Copeland also suffered actual injury in the form of damages to and diminution in the value of her PII and PCD — a form of intangible property that she entrusted to Defendants for the purpose of processing transactions, which was compromised in and as a result of the Data Breach.

171. Plaintiff Copeland suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

172. Plaintiff Copeland has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII and PCD, particularly her sensitive purchases in combination with her home address, being placed in the hands of criminals who may be interested in stealing a firearm.

173. Defendants obtained and continue to maintain Plaintiff Copeland's PII and PCD and have a continuing legal duty and obligation to protect that PII and PCD from unauthorized access and disclosure. Defendants required the PII and PCD from Plaintiff Copeland when she purchased items from Ruger's website. Plaintiff Copeland, however, would not have entrusted her PII and PCD to Defendants had she known that they would fail to maintain adequate data security. Plaintiff Copeland's PII and PCD were compromised and disclosed as a result of the Data Breach.

174. As a result of the Data Breach, Plaintiff Copeland 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 Copeland is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Lee Woods

175. During the relevant period, Plaintiff Woods purchased multiple items from the ShopRuger.com website, which was hosted on Defendant Freestyle's servers.

176. Plaintiff Woods used his debit/credit cards to purchase these items.

177. Subsequent to making this purchase, Plaintiff Woods received a letter dated August 18, 2022 from Ruger informing Plaintiff Woods that he was the victim of Defendants' Data Breach. However, this letter was sent seven months after Defendant Freestyle learned about the Data Breach.

178. The Notice Letter from Ruger informed Plaintiff Woods that Defendant Freestyle had sustained a data breach and that Plaintiff Woods' PII and PCD were captured and compromised as a result of the Data Breach.

179. The Notice Letter indicated that the ShopRuger.com website was hosted on Defendant Freestyle's servers.

180. Plaintiff Copeland's PII and PCD were likely stolen and are likely in the hands of cybercriminals who illegally accessed Defendants' network for the specific purpose of targeting the PII and PCD.

181. Plaintiff Woods typically takes measures to protect his PII and PCD and is very careful about sharing his PII and PCD.

182. As a result of the Data Breach, Plaintiff Woods has spent and continues to spend a considerable amount of time on issues related to this Data Breach. This is time that was lost and unproductive and took away from other activities and duties.

183. As a result of the Data Breach, Plaintiff Woods made reasonable efforts to mitigate the impact of the Data Breach after receiving the Notice Letter.

184. Plaintiff Woods also suffered actual injury in the form of damages to and diminution in the value of his PII and PCD — a form of intangible property that he entrusted to

Defendants for the purpose of processing transactions, which was compromised in and as a result of the Data Breach.

185. Plaintiff Woods suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

186. Plaintiff Woods has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PCD, particularly his sensitive purchases in combination with his home address, being placed in the hands of criminals who may be interested in stealing a firearm.

187. Defendants obtained and continue to maintain Plaintiff Woods' PII and PCD and have a continuing legal duty and obligation to protect that PII and PCD from unauthorized access and disclosure. Defendants required the PII and PCD from Plaintiff Woods when he made purchases from Ruger's website. Plaintiff Woods, however, would not have entrusted his PII and PCD to Defendants had he known that they would fail to maintain adequate data security. Plaintiff Woods' PII and PCD were compromised and disclosed as a result of the Data Breach.

188. As a result of the Data Breach, Plaintiff Woods 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 Woods 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

189. Plaintiffs bring this nationwide class action on behalf of themselves and all others similarly situated individuals under Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

190. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

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

191. Excluded from the Class are Defendants' officers and directors; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Also excluded from the Class are members of the judiciary to whom this case is assigned, their families, and members of their staff.

192. Plaintiffs reserve the right to amend or modify the Class definition and/or create additional subclasses as this case progresses.

193. 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 Plaintiffs at this time, based on information and belief, the Class consists of at least 167,963[28] current and former customers of Ruger whose sensitive data was compromised in the Data Breach.

194. 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 Defendants unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

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

[28] 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 Jan. 16, 2023).

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

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

e. Whether Defendants owed a duty to Class Members to safeguard their PII and PCD;

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

g. Whether Defendants knew or should have known that Freestyle's data security systems and monitoring processes were deficient;

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

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

j. Whether Defendants' conduct was negligent;

k. Whether Ruger negligently supervised Freestyle's activities as its agent;

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

m. Whether Defendants breached implied or express contracts with Plaintiffs and Class Members;

n. Whether Defendants were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;

o. Whether Defendants failed to provide notice of the Data Breach in a timely manner; and

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

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

196. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members and have no interests antagonistic to those of other Class Members. Plaintiffs' counsel are competent and experienced in litigating Class actions.

197. Predominance. Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members in that all of the Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendants' 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.

198. 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 would be 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 Defendants. 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.

199. Defendants have acted on grounds that apply generally to the Class as a whole such that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

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

200. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

201. Ruger solicited and gathered the Private Information, including the PII and PCD, of Plaintiffs and Class Members to facilitate sales transactions.

202. Freestyle built and operated a web hosting and purchase management software product that was designed and intended to help its clients, like Ruger, acquire and process large amounts of sensitive PII and PCD from customers.

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

204. Defendants owed duties of care to Plaintiffs and the Class Members whose Private Information was entrusted to them. Defendants' duties included the following:

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

b. For Ruger to exercise reasonable care in selecting and supervising Freestyle 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 Plaintiffs and Class Members of a data breach.

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

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

207. Because Defendants knew that a breach of their systems would damage thousands of Ruger's customers, including Plaintiffs and Class Members, they had a duty to adequately protect Plaintiffs' and Class Members' Private Information.

208. Defendants owed a duty of care to not subject Plaintiffs and Class Members to an unreasonable risk of harm because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices.

209. Defendants had a duty to implement, maintain, and ensure reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' Private Information.

210. Defendants knew, or should have known, that their computer systems and security practices did not adequately safeguard the Private Information of Plaintiffs and Class Members.

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

212. Defendants breached their duties of care by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

213. Defendants breached their duties of care by failing to provide prompt notice of the data breach to the persons whose PII and PCD were compromised.

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

215. Defendants acted with reckless disregard for the rights of Plaintiffs and Class Members by failing to provide prompt and adequate notice of the Data Breach so that Plaintiffs and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the PII and PCD compromised in the Data Breach.

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

217. Defendants' own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their PII and PCD. Defendants' misconduct included failing to:

a. Secure the ShopRuger.com e-commerce website;

b. Secure access to Ruger's and Freestyle's servers;

c. Audit and monitor Freestyle's actions on behalf of Ruger;

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 would provide 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.

218. Defendants also had independent duties under the FTC Act and state laws that required them to reasonably safeguard Plaintiffs' and the Class Members' PII and PCD and promptly notify them about the Data Breach.

219. Defendants breached the duties they owed to Plaintiffs 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 Plaintiffs' and Class Members' 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 Plaintiffs and Class Members had been improperly acquired or accessed.

220. But for Defendants' wrongful and negligent breach of the duties they owed Plaintiffs and Class Members, Plaintiffs' and Class Members' PII and PCD either would not have been compromised or Defendants would have been able to prevent some or all of their damages.

221. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered damages and are at imminent risk of further harm.

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

223. The injury and harm that Plaintiffs and Class Members suffered (as alleged above) was the direct and proximate result of Defendants' negligent conduct.

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

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

225. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

226. When Plaintiffs and Class Members provided their PII and PCD to Ruger when making purchases on its website, including by Plaintiffs and Class Members paying for services and/or receiving goods from Ruger, they entered into actual or implied contracts under which Ruger agreed to protect their PII and PCD and timely notify them in the event of a data breach.

227. Ruger subcontracted with Freestyle to provide a portion of Ruger's contractual duties with Plaintiffs and the Class Members, including the fulfillment of certain security obligations and notice obligations, which created an implied contract between Plaintiffs and the Class Members on one hand, and Freestyle on the other hand.

228. Defendants invited Ruger's customers, including Plaintiffs and Class Members, to make purchases on its website using payment cards in order to increase sales by making purchases more convenient.

229. An implicit part of the offer was that Defendants would safeguard Plaintiffs' and Class Members' PII and PCD using reasonable or industry-standard means and would timely notify Plaintiffs and Class Members of a data breach.

230. Ruger also affirmatively represented in its Privacy Policy that it protected the PII and PCD of Plaintiffs and Class Members in several ways, as described above.

231. Based on the implicit understanding and also on Ruger's representations, Plaintiffs and Class Members accepted the offers and provided Defendants 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.

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

233. Defendants further demonstrated an intent to safeguard the Private Information of Plaintiffs and Class Members through their conduct when they accepted Plaintiffs' and Class Members' PII and PCD. No reasonable person would provide sensitive, non-public financial information to a retailer without the implicit understanding that the retailer would maintain that information as confidential.

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

235. Plaintiffs and Class Members would not have provided their PII and PCD to Ruger and Freestyle had they known that Defendants would not safeguard their PII and PCD as promised and would not provide timely notice of a data breach.

236. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Ruger.

237. Defendants breached the express and implied contracts by failing to safeguard Plaintiffs' and Class Members' Private Information and by failing to provide Plaintiffs and Class Members with timely and accurate notice when their Private Information was compromised in the Data Breach.

238. The losses and damages Plaintiffs and Class Members sustained (as described above) were the direct and proximate result of Defendants' breaches of their express and implied contracts with Plaintiffs and Class Members.

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

239. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

240. This claim is brought in the alternative to Plaintiffs' claim for breach of express and implied contract.

241. Upon information and belief, Defendants fund their data security measures entirely from their general revenue, including payments made by Plaintiffs and Class Members.

242. Upon information and belief, Ruger paid Freestyle a fee for its services based in whole or in part on the volume of customers coming to its ShopRuger.com website. Therefore, a portion of the money Plaintiffs and the Class members paid to Ruger was used to pay Freestyle.

243. As such, a portion of the payments made by Plaintiffs 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 Defendants.

244. ShopRuger.com only accepts electronic payments. Thus, all customers who made purchases from ShopRuger.com required a reasonable level of data security.

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

246. Defendants knew that Plaintiffs and Class Members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

247. In particular, Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information and instead directed those funds to their own profits. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants increased their own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' decision to prioritize their own profits over the requisite security.

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

249. Defendants failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

250. Plaintiffs and Class Members have no adequate remedy at law.

251. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred on them.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

A. For an order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing Plaintiffs as Class Representatives, and appointing their counsel as Class counsel, and finding that Plaintiffs are proper representatives of the Class requested herein;

B. Judgment in favor of Plaintiffs and Class Members, awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, attorney's fees, statutory costs, expenses as allowable by law, and such other and further relief as is just and proper, including pre-judgment and post-judgment interest;

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

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

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

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: January 20, 2023

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC

/s/ *Gary M. Klinger*
Gary M. Klinger (*pro hac vice*)
227 West Monroe Street, Suite 2100
Chicago, IL 60606
Tel.: (866) 252-0878
gklinger@milberg.com

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

Joseph P. Guglielmo (CT 27481)
SCOTT+SCOTT ATTORNEYS AT LAW LLP
The Helmsley Building
230 Park Avenue, 17th Floor
New York, NY 10169
Tel.: 212-223-6444
Fax: 212-223-6334
jguglielmo@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

Mason A. Barney (*pro hac vice* forthcoming)
Steven D. Cohen (*pro hac vice* forthcoming)
SIRI & GLIMSTAD LLP
745 Fifth Ave, Suite 500
New York, NY 10151
Tel.: (212) 532-1091
mbarney@sirillp.com
scohen@sirillp.com

Attorneys for Plaintiffs and the Proposed Class

CERTIFICATION OF SERVICE

I hereby certify that on this ninth day of December 2022, a copy of the foregoing was filed electronically and served by mail on anyone unable to accept electronic filing. Notice of this filing will be sent by email to all parties by operation of the Court's electronic filing system or by mail to anyone unable to accept electronic filing as indicated on the Notice of Electronic Filing. Parties may access this filing through the Court's CM/ECF System.

/s/ Gary M. Klinger
Gary M. Klinger