UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH CAROLINA
AIKEN DIVISION

LATAVEIA ALLEN, *on behalf of herself and all others similarly situated*, Plaintiff, v. SRP FEDERAL CREDIT UNION, Defendant.	Case No.: 1:24-cv-07476-CMC (lead case)
NORMAN BLACK, *on behalf of himself and all others similarly situated,* Plaintiff, v. SRP FEDERAL CREDIT UNION, Defendant.	Case No. 1:24-cv-07519-CMC
GE-QUOIA WHITFIELD, *on behalf of herself and all others similarly situated*, Plaintiff, v. SRP FEDERAL CREDIT UNION, Defendant.	Case No. 1:24-cv-07537-CMC

ROSEMARY ORTIZ, *on behalf of herself and all others similarly situated*, Plaintiff, v. SRP FEDERAL CREDIT UNION, Defendant.	Case No.: 1:24-cv-07671-CMC
THERESA MCGRIER, *on behalf of herself and all others similarly situated*, Plaintiff, v. SRP FEDERAL CREDIT UNION, Defendant.	Case No.: 1:24-cv-07695-CMC
SHANNON DUNN, *on behalf of herself and all others similarly situated*, Plaintiff, v. SRP FEDERAL CREDIT UNION, Defendant.	Case No.: 1:25-cv-00210-CMC

RICKY CHASE, *on behalf of himself and all others similarly situated*, Plaintiff, v. SRP FEDERAL CREDIT UNION, Defendant.	Case No.: 1:25-cv-00312-CMC

AMENDED CONSOLIDATED CLASS ACTION COMPLAINT
JURY TRIAL DEMANDED

Plaintiffs Lataveia Allen, Shannon Dunn, Theresa McGrier, Ricky Chase, Norman Black, Ge-Quoia Whitfield, and Rosemary Ortiz ("Plaintiffs"), on behalf of themselves and all others similarly situated, state as follows for their amended consolidated class action complaint against Defendant, SRP Federal Credit Union ("SRP" or "Defendant"):

INTRODUCTION

1. Between September 5, 2024 and November 4, 2024, SRP, a credit union headquartered in South Carolina, discovered it had lost control over its computer network and the highly sensitive personal information stored on its computer network in a data breach perpetrated by cybercriminals ("Data Breach"). Upon information and belief, the Data Breach has impacted over 240,000 of Defendant's current and former customers.

2. Following an internal investigation, Defendant learned cybercriminals had gained unauthorized access to customers' personally identifiable information ("PII"), including but not limited to names, Social Security numbers, financial account information, and dates of birth.

3. Not only did cybercriminals gain unauthorized access to this PII, but they stole the information and published it on the Dark Web, where it remains available for download by anyone,

including cybercriminals. The PII available on the Dark Web includes the full credit report of SRP members, including their credit scores and account numbers, and Social Security numbers. As a result, the stolen PII could be used at any moment to commit fraud or identity theft, affecting Plaintiffs and the Class.

4. The Data Breach allowed cybercriminals unfettered access to Plaintiffs' and Class Members' most sensitive information for an appalling 60 days. Due to intentionally obfuscating language, it is unclear when Defendant finally discovered the Data Breach.

5. On or about December 12, 2024, SRP finally began notifying Class Members about the Data Breach ("Breach Notice"). A sample Breach Notice is attached as **Exhibit A**. Plaintiffs' Breach Notices are attached as **Exhibit B.**

6. Upon information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity, failed to adequately monitor its agents, contractors, vendors, and suppliers in handling and securing the PII of Plaintiffs, and failed to maintain reasonable security safeguards or protocols to protect the Class's PII—rendering it an easy target for cybercriminals.

7. Defendant's Breach Notice obfuscated the nature of the breach and the threat it posed—refusing to tell its customers how many people were impacted, how the breach happened, the identity of the cybercriminals responsible for the Data Breach, when the breach was discovered, or why Defendant delayed notifying victims that cybercriminals had gained access to their highly private information.

8. Defendant's failure to timely report the Data Breach made the victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

9. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

10. In failing to adequately protect its customers' information, adequately notify them about the breach, and obfuscating the nature of the breach, Defendant violated state law and harmed an unknown number of its current and former customers.

11. Plaintiffs and the Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiffs and members of the proposed Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

12. Plaintiffs are customers of Defendant and Data Breach victims.

13. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before the Data Breach, the private information of Plaintiffs and the Class was exactly that—private. Not anymore. Now, their private information is permanently exposed and unsecure.

PARTIES

14. Plaintiff Shannon Dunn is a natural person and citizen of Georgia where she intends to remain.

15. Plaintiff Theresa McGrier is a natural person and citizen of Georgia where she intends to remain.

16. Plaintiff Ricky Chase is a natural person and citizen of Georgia where he intends to remain.

17. Plaintiff Norman Black is a natural person and citizen of South Carolina where he intends to remain.

18. Plaintiff Lataveia Allen is a natural person and citizen of South Carolina where she intends to remain.

19. Plaintiff Ge-Quoia Whitfield in a natural person and citizen of Georgia where she intends to remain.

20. Plaintiff Rosemary Ortiz is a natural person and citizen of South Carolina where she intends to remain.

21. Defendant, SRP, is a federally chartered credit union, with its principal place of business located at 1070 Edgefield Rd, North Augusta, SC 29860. It has branches in South Carolina and Georgia, currently serving over 195,000 members throughout the United States, and has over $1.8 billion in assets.

JURISDICTION & VENUE

22. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. At least one class member and Defendant are of different states. And there are over 240,000 putative Class members.

23. This Court has personal jurisdiction over Defendant because it is headquartered in South Carolina, regularly conducts business in South Carolina, and has sufficient minimum contacts in South Carolina.

24. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

SRP

25. SRP touts that "we exist to make the people we serve and the communities we serve better. We are improving lives!"[1] It boasts an annual revenue of $19 million.[2]

26. SRP offers a wide range of products and services through their wholesale and consumer businesses, including consumer and small business banking, commercial banking, corporate and investment banking, wealth management, payments, and specialized lending businesses

27. On information and belief, SRP accumulates highly private PII of its current and former customers who bank, borrow, and invest.

28. In collecting and maintaining its customers' PII, Defendant agreed it would safeguard the data in accordance with state law and federal law. After all, Plaintiffs and Class Members themselves took reasonable steps to secure their PII.

29. SRP understood the need to protect its current and former customers' PII and prioritize its data security.

30. Despite recognizing its duty to do so, on information and belief, SRP has not implemented reasonable cybersecurity safeguards or policies to protect customers' PII or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to customers' PII.

---

[1] SRP, https://srpfcu.org/about/ (last visited March 28, 2025).

[2] SRP, https://www.jdsupra.com/legalnews/srp-federal-credit-union-announces-data-3936788/#:~:text=More%20Information%20About%20SRP%20Federal%20Credit%20Union&text=SRP%20Federal%20Credit%20Union%20employs,%2419%20million%20in%20annual%20revenue. (last visited March 28, 2025).

SRP Fails to Safeguard Customers' PII

31. Plaintiffs and Class Members are customers of SRP.

32. As a condition of receiving services from SRP, Plaintiffs and Class Members provided Defendant with their PII, including but not limited to their names, Social Security numbers, dates of birth, and other financial account information. Defendant used that PII to facilitate its services to Plaintiffs and Class Members and required Plaintiffs and Class Members to provide that PII to obtain financial services.

33. On information and belief, SRP collects and maintains customers' unencrypted PII in its computer systems.

34. In collecting and maintaining PII, Defendant implicitly agreed that it will safeguard the data using reasonable means according to state and federal law.

35. According to the Breach Notice, Defendant admits that "recently", it discovered "suspicious activity in our computer network" between "September 5, 2024, and November 4, 2024." However, due to intentionally bisecting language, it is unclear when Defendant discovered this 60-day long breach. Following an internal investigation, Defendant admitted that the unauthorized individual "potentially acquired certain files from our network during that time." Ex. A.

36. In other words, Defendant's cyber and data security systems were completely inadequate in that it not only allowed cybercriminals to obtain files containing a treasure trove of over 240,000 of its customers' highly sensitive PII, but it also did not detect the Data Breach during its occurrence, allowing cybercriminals unfettered access to Plaintiffs' and the Class's PII for an appalling 60 days.

37. Through its inadequate security practices, Defendant exposed Plaintiffs' and the

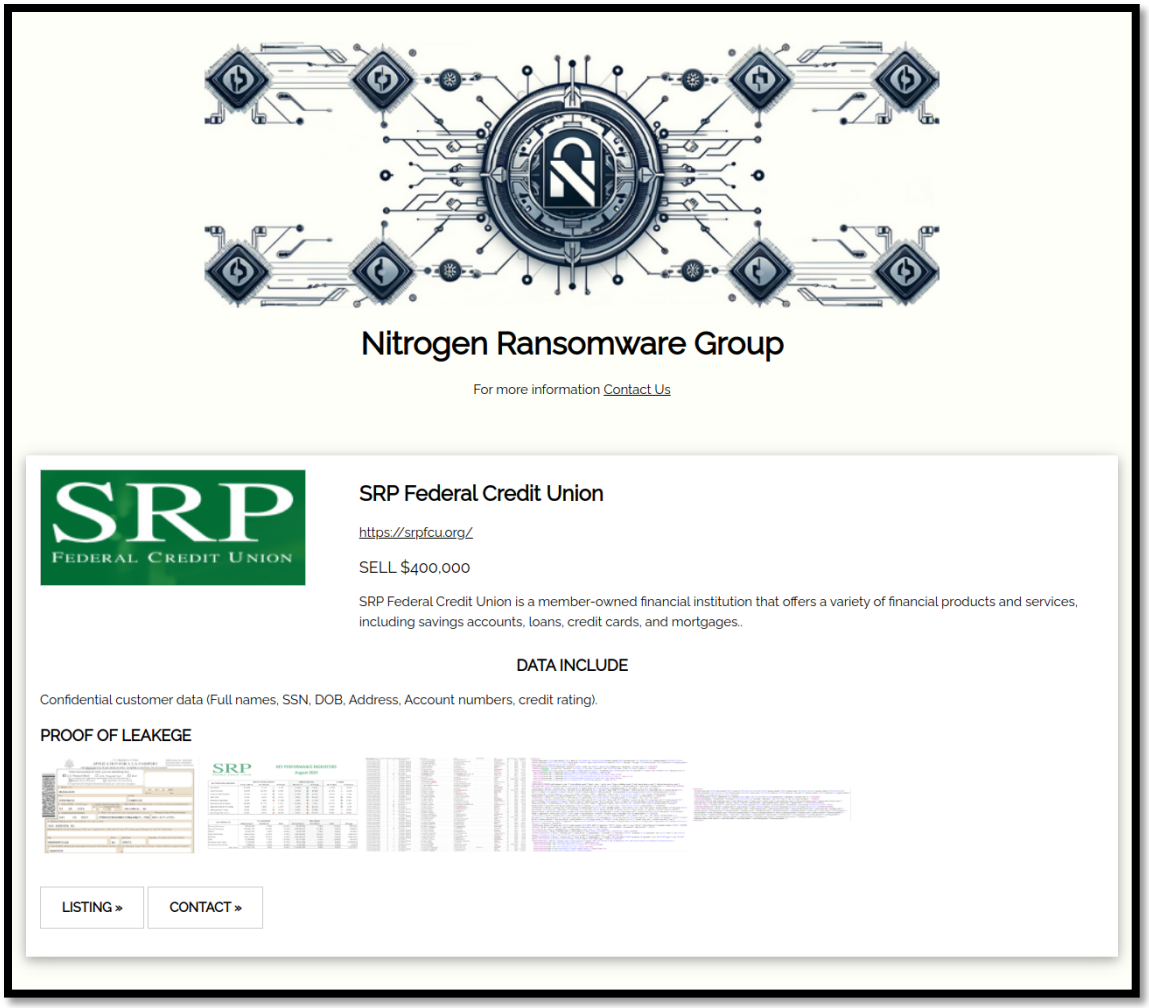
Class's PII for theft and sale on the dark web.

38. Despite its duties to safeguard PII, Defendant did not in fact follow industry standard practices in securing their customers' PII, as evidenced by the Data Breach.

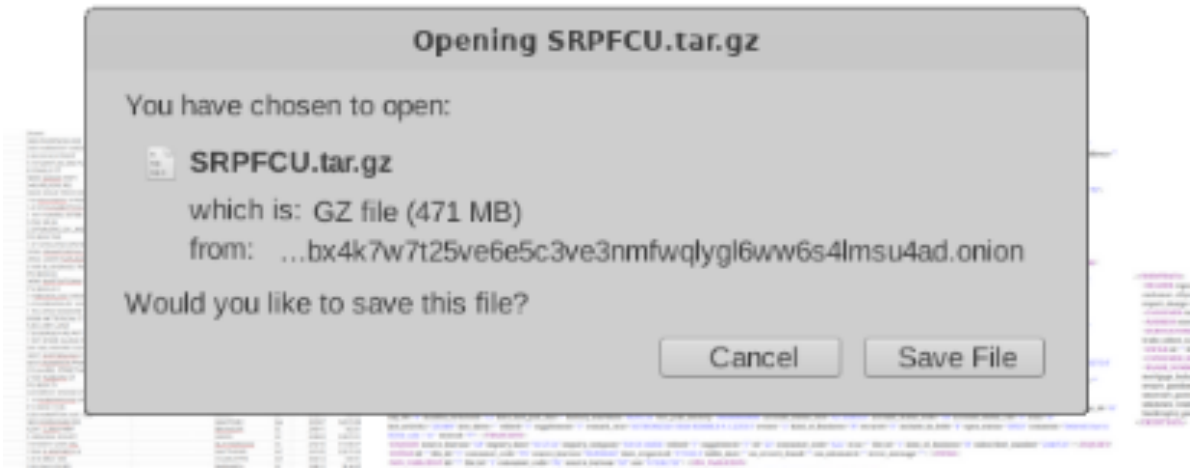
39. Upon information and belief, Nitrogen Ransomware Group was responsible for the cyberattack. Nitrogen is an incredibly notorious ransomware actor, having perpetrated multiple high-profile breaches this year alone.[3] Defendant, an alleged leader in its field, knew or should have known of the tactics that groups like Nitrogen employ.

40. With the PII secured and stolen by Nitrogen, the hackers then purportedly issued a ransom demand to Defendant. However, Defendant has provided no public information on the ransom demand or payment.

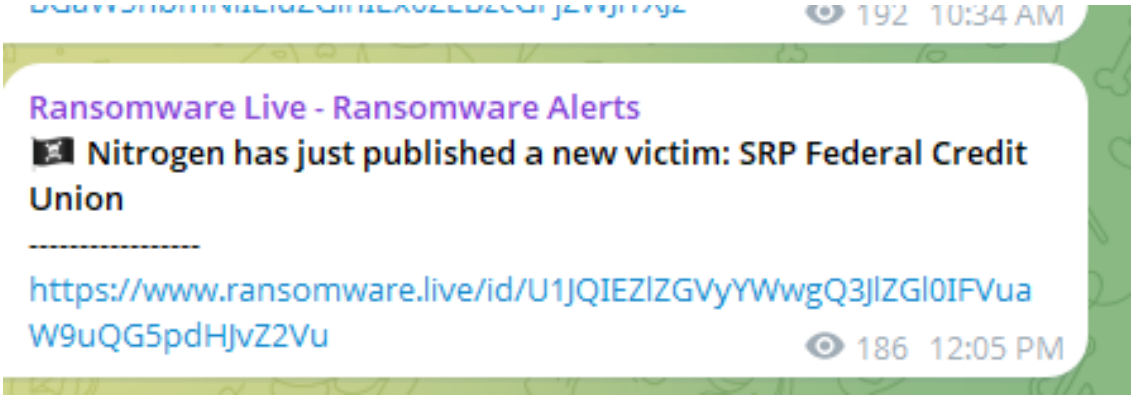
[3] Halcyon, Emerging Threat Actor, https://www.halcyon.ai/attacks-news/emerging-threat-actor-nitrogen-ransomware (last visited March 28, 2025).



41. As a result of Defendant's inadequate cybersecurity, Nitrogen not only accessed and ransomed Plaintiffs' and the Class's PII, but actually stole at least 650 GB of information and published at least 471 MB of that stolen information on its leak site as of October 2025. The stolen and published information includes identifiable SRP customer records, including their full credit reports, and internal documentation containing PII.



[4]



[4] Posted on Telegram for Ransomware Live on 12/04/2024.

42. For example, the published data includes items such as: client spreadsheets listing full names, account numbers, Social Security numbers, and balances; credit-rating and performance reports summarizing member financial risk metrics; and customer address and phone data combined with credit scores and dates of birth.

43. The cybercriminals' post includes downloadable archives of SRP member data, including the PII of at least Plaintiffs Allen, Whitfield, McGrier, Dunn, and Chase. On information and belief, Plaintiffs Black and Ortiz have also had their stolen PII published on the dark web.

44. Although the entire stolen data set is not currently published on Nitrogen's leak site, on information and belief, Nitrogen still has possession of a much larger dataset that it could publish at any time.

45. Ransomware attacks, like that experienced by Defendant, are frequently leveraged by cybercriminals to extort a ransom from the entities from which they steal consumer data in exchange for a promise to delete that data. However, often criminals will accept a ransom payment, falsify evidence of deletion, and then sell personal data on the dark web. For example, recently United Healthcare paid a $22 million dollar ransom in exchange for proof of deletion only to find that the patient data exfiltrated in the cyberattack was subsequently being sold on the dark web.[5]

46. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data."[6] This publication also explains that "[t]he FBI does

[5] *After paying a $22M ransom to delete it, data stolen in Change HealthCare breach resurfaces*, accessible at, https://www.comparitech.com/news/after-paying-a-22m-ransom-to-delete-it-data-stolen-in-change-healthcare-breach-resurfaces/

[6] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware

not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."[7]

47. Companies should treat ransomware attacks as any other data breach incident because ransomware attacks don't just hold networks hostage, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[8] As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence […] the initial assumption should be that data may have been exfiltrated."

48. An increasingly prevalent form of ransomware attack is the "encryption+exfiltration" attack in which the attacker encrypts a network and exfiltrates the data contained within.[9] In 2020, over 50% of ransomware attackers exfiltrated data from a network before encrypting it.[10] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[11] And even where companies pay for the return of data attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[12]

49. On or around December 12, 2024 – at least three months after the Data Breach first

---

[7] *Id.*

[8] *Ransomware: The Data Exfiltration and Double Extortion Trends*, available at https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends

[9] *The chance of data being stolen in a ransomware attack is greater than one in ten*, available at https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/

[10] 2020 Ransomware Marketplace Report, available at https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report

[11] *Id*.

[12] *Id*.

occurred – Defendant finally notified Plaintiffs and Class Members about the Data Breach.

50. In response to the Data Breach, Defendant contends that it will be "enhancing our technical security measures." Ex. A. Although Defendant fails to expand on what these alleged "enhancements" are, such enhancements should have been in place before the Data Breach.

51. Through its Breach Notice, Defendant recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "remain vigilant to protect against potential fraud and/or identity theft" Ex. A.

52. Through the Data Breach, Defendant recognized its duty to implement reasonable cybersecurity safeguards or policies to protect customers' PII, insisting that, despite the Data Breach demonstrating otherwise, it takes the "values and respects the privacy of your personal information." Ex. A.

53. On information and belief, SRP offered several months of complimentary credit monitoring services to all victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers.

54. Even with several months of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiffs' and Class Members' PII is still substantially high. The stolen PII is currently published on the Dark Web and available for download by anyone, including cybercriminals. Thus, Plaintiffs and the Class are at present and imminent threat of suffering fraud and identity theft. Additionally, as the cybercriminals likely possess significantly more PII than what has already been published, additional stolen PII could be published at any moment.

55. Though they no doubt did in this case, cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or

misuse Plaintiffs' and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiffs' and the Class's financial accounts.

56. On information and belief, Defendant failed to adequately train its IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its customers' PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

Consumers Prioritize Data Security

57. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."[13] Therein, Cisco reported the following:

a. "For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't trust with their data."[14]

b. "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly."[15]

c. 89% of consumers stated that "I care about data privacy."[16]

d. 83% of consumers declared that "I am willing to spend time and money to protect

[13] *Privacy Awareness: Consumers Taking Charge to Protect Personal*, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited March 19, 2025).
[14] *Id*. at 3.
[15] *Id*.
[16] *Id*. at 9.

data" and that "I expect to pay more" for privacy.[17]

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[18]

f. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."[19]

The Data Breach was a Foreseeable Risk of Which Defendant was on Notice.

58. It is well known that PII, including Social Security numbers, are an invaluable commodity and a frequent target of hackers.

59. 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.[20]

60. In 2023, an all-time high for data compromises occurred, with 3,205 compromises affecting 353,027,892 total victims. The estimated number of organizations impacted by data compromises has increased by +2,600 percentage points since 2018, and the estimated number of victims has increased by +1400 percentage points. The 2023 compromises represent a 78 percentage point increase over the previous year and a 72 percentage point hike from the previous all-time high number of compromises (1,860) set in 2021.

61. In light of recent high profile data breaches at other industry leading companies, including T-Mobile, USA (37 million records, February-March 2023), 23andMe, Inc. (20 million records, October 2023), Wilton Reassurance Company (1.4 million records, June 2023), NCB

[17] *Id*.
[18] *Id*.
[19] *Id*. at 11.
[20] 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/ (last visited March 28, 2025).

Management Services, Inc. (1 million records, February 2023), Defendant knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

62. 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.

63. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

64. In the years immediately preceding the Data Breach, Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks, including ransomware attacks involving data theft, because warnings were readily available and accessible via the internet.

65. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[21]

66. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage,

[21] High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations, FBI, available at https://www.ic3.gov/Media/Y2019/PSA191002 (last visited March 28, 2025).

leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[22]

67. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[23]

68. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) ransomware actors were targeting entities such as Defendant, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities such as Defendant, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included threatening to release stolen data.

69. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted PII of over 240,000 of its current and former customers in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII and Defendant's type of business had cause to be particularly on guard against such an attack.

70. Before the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack. Notably, data breaches are prevalent in today's society

[22] Ransomware mentioned in 1,000+ SEC filings over the past year, ZDNet, https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last visited March 28, 2025).

[23] Ransomware Guide, U.S. CISA, https://www.cisa.gov/stopransomware/ransomware-guide (last visited March 28, 2025).

therefore making the risk of experiencing a data breach entirely foreseeable to Defendant.

71. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted its customers' Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

Plaintiff Shannon Dunn's Experience and Injuries

72. Plaintiff Shannon Dunn is a customer of Defendant and a Data Breach victim.

73. As a condition of receiving services from SRP, Plaintiff Dunn provided Defendant with her PII, including but not limited to her name, Social Security number, and date of birth. Defendant used that PII to facilitate its services to Plaintiff Dunn and required Plaintiff to provide that PII to obtain financial services.

74. Plaintiff Dunn provided her PII to Defendant and trusted that the company would use reasonable measures to protect it according to state and federal law.

75. Plaintiff Dunn is a victim of the Data Breach, having received notice dated December 12, 2024, stating that her name, date of birth, Social Security number, and financial account number were contained in the files stolen in the Data Breach.

76. Plaintiff Dunn's PII has already been published by cybercriminals on the Dark Web.

77. In February 2025, Plaintiff Dunn learned that she became a victim of identity theft when an unknown person submitted a W-2 using her name and Social Security number. As a result, Plaintiff has been trying to resolve the issue from February to October 2025, spending 1-2 hours per day on the phone with the IRS for long stretches of time, estimated to have taken 150-200 total hours to-date.

78. Defendant deprived Plaintiff Dunn of the earliest opportunity to guard herself

against the Data Breach's effects by failing to promptly notify her about the Breach.

79. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Dunn's PII for theft by cybercriminals and sale on the dark web. Plaintiff Dunn has already received a credit alert that an unauthorized actor was trying to access her accounts.

80. Plaintiff Dunn suffered actual injury from the exposure of her PII —which violates her rights to privacy in that it is an intrusion upon seclusion and publicity given to private life.

81. Plaintiff Dunn suffered actual injury in the form of damage to and diminution in the value of her PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

82. As a result of the Data Breach, in addition to the time spent dealing with her identity theft, Plaintiff Dunn has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing her online account passwords, and monitoring her credit information. Plaintiff Dunn purchased credit monitoring, costing her $18 per month, and has spent over ten hours investigating the breach on her own.

83. Plaintiff Dunn has already spent and will continue to spend considerable time and effort monitoring her accounts to protect herself from identity theft. Plaintiff Dunn fears for her personal financial security, uncertainty over what PII was exposed in the Data Breach, and the possibility of further identity theft. Plaintiff has and is experiencing feelings of anxiety, stress, fear, and frustration because of the Data Breach. Plaintiff is experiencing anxiety, distress, and fear regarding how this Data Breach, including the exposure and loss of her Social Security number, will impact her ability to protect herself from identity theft. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that

the law contemplates and addresses.

84. Plaintiff Dunn is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's failure to inform Plaintiff about the Data Breach in a timely fashion.

85. Indeed, following the Data Breach, Plaintiff Dunn began suffering a significant increase in spam calls and text messages posing as her bank or another financial institution.

86. On information and belief, Plaintiff Dunn's phone number and email were compromised as a result of the Data Breach.

87. Plaintiff Dunn has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Theresa McGrier's Experience and Injuries

88. Plaintiff Theresa McGrier is a customer of Defendant and a data breach victim.

89. As a condition of receiving services from SRP, Plaintiff McGrier provided Defendant with her PII, including but not limited to her name, Social Security number, and date of birth. Defendant used that PII to facilitate its services to Plaintiff and required Plaintiff to provide that PII to obtain financial services.

90. Plaintiff McGrier provided her PII to Defendant and trusted that the company would use reasonable measures to protect it according to state and federal law.

91. Plaintiff McGrier is a victim of the Data Breach, having received notice dated December 12, 2024, stating that her name, date of birth, Social Security number, credit card number, and financial account number were contained in the files stolen in the Data Breach.

92. Plaintiff McGrier's PII has already been published by cybercriminals on the Dark Web.

93. Defendant deprived Plaintiff McGrier of the earliest opportunity to guard herself against the Data Breach's effects by failing to promptly notify her about the Breach.

94. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff McGrier's PII for theft by cybercriminals and sale on the dark web.

95. Plaintiff McGrier suffered actual injury from the exposure of her PII —which violates her rights to privacy in that it is an intrusion upon seclusion and publicity given to private life.

96. Plaintiff McGrier suffered actual injury in the form of damages to and diminution in the value of her PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

97. As a result of the Data Breach, Plaintiff McGrier has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements daily, changing account passwords and monitoring her credit information. After the Data Breach occurred, Plaintiff McGrier suffered a number of fraudulent charges on her SRP account, forcing her to cancel her SRP debit card and get a new card issued. This also forced Plaintiff McGrier to spend time updating her payment methods for numerous accounts that were linked to her SRP debit card to avoid late charges and/or missed payments.

98. Plaintiff McGrier has already spent and will continue to spend considerable time and effort monitoring her accounts to protect herself from identity theft. Plaintiff McGrier fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach.

Plaintiff has and is experiencing feelings of anxiety, stress, fear, and frustration because of the Data Breach. Plaintiff McGrier is experiencing anxiety, distress, and fear regarding how this Data Breach, including the exposure and loss of her Social Security number, will impact her ability to protect herself from identity theft. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

99. Plaintiff McGrier is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's failure to inform Plaintiff about the Data Breach in a timely fashion.

100. Indeed, following the Data Breach, Plaintiff McGrier also began suffering a significant increase in spam calls, text messages, and emails posing as SRP or other financial institutions. This spam suggests that her PII is now in the hands of cybercriminals.

101. On information and belief, Plaintiff McGrier's phone number and email, were compromised as a result of the Data Breach.

102. Plaintiff McGrier has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Ricky Chase's Experience and Injuries

103. Plaintiff Ricky Chase is a customer of Defendant and a data breach victim.

104. As a condition of receiving services from SRP, Plaintiff Chase provided Defendant with his PII, including but not limited to his name, Social Security number, and date of birth. Defendant used that PII to facilitate its services to Plaintiff Chase and required Plaintiff to provide

that PII to obtain financial services.

105. Plaintiff Chase provided his PII to Defendant and trusted that the company would use reasonable measures to protect it according to state and federal law.

106. Plaintiff Chase is a victim of the Data Breach, having received notice dated December 12, 2024, stating that his name, date of birth, Social Security number, and financial account number were contained in the files stolen in the Data Breach.

107. Plaintiff Chase's PII has already been published by cybercriminals on the Dark Web.

108. Defendant deprived Plaintiff Chase of the earliest opportunity to guard himself against the Data Breach's effects by failing to promptly notify him about the Breach.

109. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Chase's PII for theft by cybercriminals and sale on the dark web.

110. Plaintiff Chase suffered actual injury from the exposure of his PII —which violates his rights to privacy in that it is an intrusion upon seclusion and publicity given to private life.

111. Plaintiff Chase suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

112. As a result of the Data Breach, Plaintiff Chase has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, resetting his online credentials, and monitoring his credit information. Plaintiff Chase has flagged multiple unauthorized charges on his accounts associated with SRP.

113. Plaintiff Chase has already spent and will continue to spend considerable time and

effort monitoring his accounts to protect himself from identity theft. To date, Plaintiff Chase has spent over 20 hours attempting to remedy the harms from the Data Breach. Plaintiff fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, stress, fear, and frustration because of the Data Breach. Plaintiff is experiencing anxiety, distress, and fear regarding how this Data Breach, including the exposure and loss of his Social Security number, will impact his ability to protect himself from identity theft. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

114. Plaintiff Chase is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's failure to inform Plaintiff about the Data Breach in a timely fashion.

115. Indeed, following the Data Breach, Plaintiff Chase began suffering a significant increase in spam calls and emails posing as his bank or another financial institution. These spam calls and emails suggest that his PII is now in the hands of cybercriminals.

116. On information and belief, Plaintiff Chase's phone number and email, were compromised as a result of the Data Breach.

117. Plaintiff Chase has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Norman Black's Experience and Injuries

118. Plaintiff Norman Black is a customer of Defendant and a data breach victim. Plaintiff Black holds multiple accounts with SRP, including a checking account and a savings

account, and has taken out auto loans through SRP. He held a debit card with SRP until December 2024.

119. As a condition of receiving services from SRP, Plaintiff Black provided Defendant with his PII, including but not limited to his name, Social Security number, and date of birth. Defendant used that PII to facilitate its services to Plaintiff and required Plaintiff to provide that PII to obtain financial services.

120. Plaintiff Black is a victim of the Data Breach, having received notice dated December 12, 2024, stating that his name, date of birth, Social Security number, and financial account number were contained in the files stolen in the Data Breach.

121. Plaintiff Black provided his PII to Defendant and trusted that the company would use reasonable measures to protect it according to state and federal law.

122. On information and belief, Plaintiff Black's PII has already been published by cybercriminals on the Dark Web.

123. Defendant deprived Plaintiff Black of the earliest opportunity to guard himself against the Data Breach's effects by failing to promptly notify him about the Breach.

124. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Black's PII for theft by cybercriminals and sale on the dark web.

125. Plaintiff Black suffered actual injury from the exposure of his PII —which violates his rights to privacy in that it is an intrusion upon seclusion and publicity given to private life.

126. Plaintiff Black suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

127. In approximately October of 2024, Plaintiff Black began receiving text

notifications that log-in attempts were being made on his online SRP accounts and online credit card accounts. Neither he nor any authorized account holders made these login attempts, and thus, on information and belief, his PII that was stolen in the Data Breach was being used to commit identity theft and attempted fraud.

128. Then, in August 2025, someone fraudulently used Plaintiff Black's SRP checking account to make a $69.99 purchase. As a result, Plaintiff Black had to obtain a new debit card for that account.

129. As a result of the Data Breach, Plaintiff Black has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, changing passwords, reviewing credit card and financial account statements, monitoring his credit information, and ultimately closing his SRP account and opening another due to various fraudulent charges on his account.

130. Plaintiff Black has already spent and will continue to spend considerable time and effort monitoring his accounts to protect himself from identity theft. Plaintiff fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff Black has and is experiencing feelings of anxiety, stress, fear, and frustration because of the Data Breach. Plaintiff is experiencing anxiety, distress, and fear regarding how this Data Breach, including the exposure and loss of his Social Security number, will impact his ability to protect himself from identity theft. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

131. Plaintiff Black is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's failure to inform Plaintiff about the Data Breach in a

timely fashion.

132. Indeed, following the Data Breach, in addition to the unauthorized charges, Plaintiff Black began suffering a significant increase in spam calls and emails posing as his bank or another financial institution. These spam calls and emails suggest that his PII is now in the hands of cybercriminals.

133. On information and belief, Plaintiff Black's phone number and email, were compromised as a result of the Data Breach.

134. Plaintiff Black has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Lataveia Allen's Experience and Injuries

135. Plaintiff Lataveia Allen is a customer of Defendant and a data breach victim.

136. As a condition of receiving services from SRP, Plaintiff Allen provided Defendant with her PII, including but not limited to her name, Social Security number, and date of birth. Defendant used that PII to facilitate its services to Plaintiff and required Plaintiff to provide that PII to obtain financial services.

137. Plaintiff Allen provided her PII to Defendant and trusted that the company would use reasonable measures to protect it according to state and federal law.

138. Plaintiff Allen is a victim of the Data Breach, having received notice from Defendant dated December 12, 2024, stating that her name, date of birth, Social Security number, and financial account number were contained in the files stolen in the Data Breach.

139. Plaintiff Allen's PII has already been published by cybercriminals on the Dark Web. After the Data Breach, Plaintiff Allen received a dark web notification from her credit and

identity theft protection service, Credit Karma, informing her that her PII was found on the dark web.

140. Defendant deprived Plaintiff Allen of the earliest opportunity to guard herself against the Data Breach's effects by failing to promptly notify her about the Breach.

141. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Allen's PII for theft by cybercriminals and sale on the dark web.

142. Plaintiff Allen suffered actual injury from the exposure of her PII —which violates her rights to privacy in that it is an intrusion upon seclusion and publicity given to private life.

143. Plaintiff Allen suffered actual injury in the form of damages to and diminution in the value of her PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

144. As a result of the Data Breach, Plaintiff has spent hours of her time on reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing her credit card and financial account statements, placing a credit freeze through credit bureaus, and monitoring her credit information.

145. Plaintiff Allen has already spent and will continue to spend considerable time and effort monitoring her accounts to protect herself from identity theft. Plaintiff Allen fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, stress, fear, and frustration because of the Data Breach. Plaintiff Allen is experiencing extreme anxiety, distress, and fear regarding how this Data Breach, including the exposure and loss of her Social Security number, will impact her ability to protect herself from identity theft. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

146. Plaintiff Allen is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's failure to inform Plaintiff Allen about the Data Breach in a timely fashion.

147. Indeed, following the Data Breach, Plaintiff Allen began suffering a significant increase in spam calls, text messages, and emails about purported unpaid fees or debts, and the spammers almost always ask Plaintiff Allen for her financial account information and other PII. These spam calls and messages suggest that her PII is now in the hands of cybercriminals. The spam calls became so frequent that Plaintiff Allen put a call block on her phone.

148. On information and belief, Plaintiff Allen's phone number and email were compromised as a result of the Data Breach as she provided that information to Defendant.

149. Plaintiff Allen has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Ge-Quoia Whitfield's Experience and Injuries

150. Plaintiff Ge-Quoia Whitfield is a customer of Defendant and a data breach victim.

151. As a condition of receiving services from SRP, Plaintiff Whitfield provided Defendant with her PII, including but not limited to her name, Social Security number, and date of birth. Defendant used that PII to facilitate its services to Plaintiff and required Plaintiff to provide that PII to obtain financial services.

152. Plaintiff Whitfield provided her PII to Defendant and trusted that the company would use reasonable measures to protect it according to state and federal law.

153. Plaintiff Whitfield is a victim of the Data Breach, having received notice dated

December 12, 2024, stating that her name, date of birth, Social Security number, and financial account number were contained in the files stolen in the Data Breach.

154. Plaintiff Whitfield's PII has already been published— by cybercriminals on the Dark Web. Plaintiff Whitfield's credit monitoring services indicated that she was a victim of this Data Breach.

155. Defendant deprived Plaintiff Whitfield of the earliest opportunity to guard herself against the Data Breach's effects by failing to promptly notify her about the Breach.

156. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Whitfield's PII for theft by cybercriminals and sale on the dark web.

157. Plaintiff Whitfield suffered actual injury from the exposure of her PII—which violates her rights to privacy in that it is an intrusion upon seclusion and publicity given to private life.

158. Plaintiff Whitfield suffered actual injury in the form of damages to and diminution in the value of her PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

159. As a result of the Data Breach, Plaintiff Whitfield has received a noticeable increase in spam calls and emails since September 2024. Plaintiff Whitfield receives spam emails, including phishing attempts asking her to click on an external link, daily. Furthermore, Plaintiff receives spam calls at least once per day.

160. Additionally, as a result of the Data Breach, Plaintiff Whitfield has received an increase in dark web notifications. These notifications occur approximately once per month, stating that her name, email, and phone number have been found on the dark web. This activity did not take place prior to the breach.

161. As a result of the Data Breach, Plaintiff Whitfield has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements on a daily basis, and monitoring her credit information.

162. Plaintiff Whitfield has already spent and will continue to spend considerable time and effort monitoring her accounts on a daily basis to protect herself from identity theft. Plaintiff Whitfield fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff Whitfield has and is experiencing feelings of anxiety, stress, fear, and frustration because of the Data Breach. Plaintiff Whitfield is experiencing anxiety, distress, and fear regarding how this Data Breach, including the exposure and loss of her Social Security number, will impact her ability to protect herself from identity theft. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

163. Plaintiff Whitfield is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's failure to inform Plaintiff Whitfield about the Data Breach in a timely fashion.

164. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Rosemary Ortiz's Experience and Injuries

165. Plaintiff Rosemary Ortiz is a customer of Defendant and a data breach victim.

166. As a condition of receiving services from SRP, Plaintiff Ortiz provided Defendant

with her PII, including but not limited to her name, Social Security number, and date of birth. Defendant used that PII to facilitate its services to Plaintiff Ortiz and required Plaintiff to provide that PII to obtain financial services.

167. Plaintiff Ortiz provided her PII to Defendant and trusted that the company would use reasonable measures to protect it according to state and federal law.

168. Plaintiff Ortiz is a victim of the Data Breach, having received notice dated December 12, 2024, stating that her name, date of birth, Social Security number, credit card number, and financial account number were contained in the files stolen in the Data Breach.

169. On information and belief, Plaintiff Ortiz's PII has already been published by cybercriminals on the Dark Web.

170. Defendant deprived Plaintiff Ortiz of the earliest opportunity to guard herself against the Data Breach's effects by failing to promptly notify her about the Breach.

171. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Ortiz's PII for theft by cybercriminals and sale on the dark web. Plaintiff Ortiz has already received a credit alert that an unauthorized actor was trying to access her accounts.

172. Plaintiff Ortiz suffered actual injury from the exposure of her PII —which violates her rights to privacy in that it is an intrusion upon seclusion and publicity given to private life.

173. Plaintiff Ortiz suffered actual injury in the form of damages to and diminution in the value of her PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

174. As a result of the Data Breach, Plaintiff Ortiz has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing her accounts, changing her online account passwords, and monitoring her credit

information. As a result of the Data Breach, Plaintiff Ortiz purchased credit monitoring, costing her $32 per month.

175. Plaintiff Ortiz has already spent and will continue to spend considerable time and effort monitoring her accounts to protect herself from identity theft. Plaintiff Ortiz fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, stress, fear, and frustration because of the Data Breach. Plaintiff is experiencing anxiety, distress, and fear regarding how this Data Breach, including the exposure and loss of her Social Security number, will impact her ability to protect herself from identity theft. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

176. Plaintiff Ortiz is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's failure to inform Plaintiff about the Data Breach in a timely fashion.

177. Indeed, following the Data Breach, Plaintiff Ortiz began suffering a significant increase in spam calls and text messages posing as her bank or another financial institution. These spam calls and texts suggest that her PII is now in the hands of cybercriminals.

178. On information and belief, Plaintiff Ortiz's phone number and email, were all information compromised as a result of the Data Breach.

179. Plaintiff Ortiz has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

180. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

181. As a result of SRP failure to prevent the Data Breach, Plaintiffs and the proposed Class Members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiffs and the Class have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

182. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

183. The value of Plaintiffs' and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

184. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover, Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

185. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

186. One such example of criminals using PII for profit is the development of "Fullz" packages.

187. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

188. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and the Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and the Class, and it

is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and members of the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

189. Defendant disclosed the PII of Plaintiffs and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiffs and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

190. Defendant's failure to properly notify Plaintiffs and the Class of the Data Breach exacerbated Plaintiffs' and the Class's injuries by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

191. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

192. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

193. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

194. The FTC recommends that companies not maintain information 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 for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

195. 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.

196. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

197. Several best practices have been identified that—at a minimum—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-

malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

198. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

199. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04).

200. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

201. Plaintiffs bring this action on behalf of themselves and all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

202. Specifically, Plaintiffs propose the following Nationwide Class and South Carolina Subclass (collectively referred to herein as the "Class"), subject to amendment as appropriate:

> **Nationwide Class**
> All individuals whose PII was accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data

Breach.

South Carolina Subclass
All individuals residing in South Carolina whose PII was accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

Georgia Subclass
All individuals residing in Georgia whose PII was accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

203. Excluded from the Class are SRP and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned, as well as their judicial staff and immediate family members.

204. Plaintiffs reserve the right to modify or amend the definition of the proposed Class, as well as add Subclass(es), before the Court determines whether certification is appropriate.

205. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

206. **Numerosity.** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of at least 240,000 former and current customers of SRP whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through SRP's records, Class Members' records, publication notice, self-identification, and other means.

207. **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 SRP engaged in the conduct alleged herein;

b. Whether SRP's conduct violated the South Carolina Data Breach Security Act, S.C. Code Ann. §§ 39-1-90, *et seq*. invoked below;

c. When SRP learned of the Data Breach;

d. Whether SRP's response to the Data Breach was adequate;

e. Whether SRP unlawfully lost or disclosed Plaintiffs' and Class Members' PII;

f. Whether SRP failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII compromised in the Data Breach;

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

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

i. Whether SRP owed a duty to Class Members to safeguard their PII;

j. Whether SRP breached its duty to Class Members to safeguard their PII;

k. Whether hackers obtained Class Members' PII via the Data Breach;

l. Whether SRP had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

m. Whether SRP breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

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

o. Whether Defendant took reasonable measures to determine the extent of the Data

Breach after discovering it;

p. What damages Plaintiffs and Class Members suffered as a result of SRP's misconduct;

q. Whether SRP's conduct was negligent;

r. Whether SRP's conduct was *per se* negligent;

s. Whether SRP was unjustly enriched;

t. Whether Plaintiffs and Class Members are entitled to actual, treble and/or statutory damages;

u. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

v. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

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

209. **Adequacy of Representation.** Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

210. **Predominance.** SRP has engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from SRP'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.

211. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. 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 SRP. In contrast, conducting 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.

212. Class certification is also appropriate because SRP has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

213. Finally, all members of the proposed Class are readily ascertainable. SRP has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by SRP.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of Plaintiffs and the Nationwide Class, or alternatively, the South Carolina Subclass and Georgia Subclass)

214. Plaintiffs restate and reallege paragraphs 1-213 above and hereafter as if fully set forth herein.

215. SRP knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' PII, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

216. SRP's duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

217. SRP knew or should have known of the risks inherent in collecting the PII of Plaintiffs and Class Members and the importance of adequate security. SRP was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

218. SRP owed a duty of care to Plaintiffs and Class Members whose PII was entrusted to it. SRP's duties included, but were not limited to, the following:

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

b. To protect customers' PII using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of PII in its possession;

d. To employ reasonable security measures and otherwise protect the PII of Plaintiffs and Class Members pursuant to the FTCA and the South Carolina Data Breach Security Act; and

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

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

220. SRP's duty also arose because Defendant was bound by industry standards to protect its customers' confidential PII.

221. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and SRP owed them a duty of care to not subject them to an unreasonable risk of harm.

222. SRP, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' PII within SRP's possession.

223. SRP, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Plaintiffs and Class Members.

224. SRP, by its actions and/or omissions, breached its duty of care by failing to

promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose PII was compromised.

225. SRP breached its duties and, thus, was negligent by failing to use reasonable measures to protect Class Members' PII, and/or by acting with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class Members' PII by. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' PII;

e. Failing to comply with the FTCA; and

f. Failing to detect in a timely manner that Class Members' PII had been compromised.

226. SRP had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust SRP with their PII was predicated on the understanding that SRP would take adequate security precautions. Moreover, only SRP had the ability to protect its systems (and the PII that it stored on them) from attack.

227. SRP's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' PII to be compromised and exfiltrated as alleged herein.

228. SRP's breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their PII, and/or loss of time and money to

monitor their accounts for fraud.

229. As a result of SRP's negligence in breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their PII, which is still in the possession of third parties, will be used for fraudulent purposes.

230. SRP also had independent duties under state laws that required it to reasonably safeguard Plaintiffs' and Class Members' PII and promptly notify them about the Data Breach.

231. As a direct and proximate result of SRP's negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

232. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

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

234. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring SRP to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On behalf of Plaintiffs and the Nationwide Class, or alternatively, the South Carolina Subclass and Georgia Subclass)

235. Plaintiffs restate and reallege paragraphs 1-213 above and hereafter as if fully set forth herein.

236. Pursuant to Section 5 of the FTCA, SRP had a duty to provide fair and adequate computer systems and data security to safeguard the PII of Plaintiffs and Class Members.

237. SRP breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

238. Plaintiffs and Class Members are within the class of persons that the FTCA is intended to protect.

239. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII (such as the PII compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of SRP's duty in this regard.

240. SRP violated the FTCA by failing to use reasonable measures to protect the PII of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

241. It was reasonably foreseeable, particularly given the growing number of data breaches of PII, that the failure to reasonably protect and secure Plaintiffs' and Class Members' PII in compliance with applicable laws would result in an unauthorized third-party gaining access to SRP's networks, databases, and computers that stored Plaintiffs' and Class Members' unencrypted PII.

242. SRP's violations of the FTCA constitute negligence *per se*.

243. Plaintiffs' and Class Members' PII constitutes personal property that was stolen due to SRP's negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

244. As a direct and proximate result of SRP's negligence *per se*, Plaintiffs and the Class

have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their PII, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

245. SRP breached its duties to Plaintiffs and the Class under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

246. As a direct and proximate result of SRP's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

247. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring SRP to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Nationwide Class, or alternatively, the South Carolina Subclass and Georgia Subclass)

248. Plaintiffs restate and reallege paragraphs 1-213 above and hereafter as if fully set forth herein.

249. SRP provides banking and financial services to Plaintiffs and Class Members. Plaintiffs and Class Members formed an implied contract with Defendant regarding the provision of those services through their collective conduct, including by Plaintiffs and Class Members accepting services from Defendant.

250. Through Defendant's offering of banking and financial services, it knew or should

have known that it must protect Plaintiffs' and Class Members' confidential PII in accordance with SRP's policies, practices, and applicable law.

251. As consideration, Plaintiffs and Class Members deposited money with SRP and turned over valuable PII to SRP. Accordingly, Plaintiffs and Class Members bargained with SRP to securely maintain and store their PII.

252. SRP accepted possession of Plaintiffs' and Class Members' PII for the purpose of providing banking and financial services to Plaintiffs and Class Members.

253. In delivering their PII to SRP and accepting banking and financial services, Plaintiffs and Class Members intended and understood that SRP would adequately safeguard the PII as part of that service.

254. Defendant's implied promises to Plaintiffs and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to PII also protect the confidentiality of that data; (2) taking steps to ensure that the PII that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the PII against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

255. Plaintiffs and Class Members would not have entrusted their PII to SRP in the absence of such an implied contract.

256. Had SRP disclosed to Plaintiffs and the Class that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and Class Members would not have provided their PII to SRP.

257. SRP recognized that Plaintiffs' and Class Member's PII is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and the other Class Members.

258. SRP violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' PII.

259. Plaintiffs and Class Members have been damaged by SRP's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT IV
VIOLATION OF THE SOUTH CAROLINA DATA BREACH SECURITY ACT
S.C. Code Ann. §§ 39-1-90, *et seq*.
(On behalf of Plaintiffs Black, Allen, and Ortiz and the South Carolina Subclass)

260. Plaintiffs Black, Allen, and Ortiz restate and reallege paragraphs 1-213 above and hereafter as if fully set forth herein.

261. SRP is a business that owns or licenses computerized data or other data that includes personal identifying information as defined by S.C. Code Ann. § 39-1-90(A).

262. Plaintiffs' and the South Carolina Subclass's PII includes personal identifying information as covered under S.C. Code Ann. § 39-1-90(D)(3).

263. SRP was required to adequately notify Plaintiffs and the South Carolina Subclass following discovery or notification of a Data Breach if PII that was not rendered unusable by cybercriminals through encryption, redaction, or other methods was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, in the most expedient time possible and without unreasonable delay under S.C. Code Ann. § 39-1-90(A).

264. Because SRP discovered the Data Breach in which the compromised PII was not rendered unusable through encryption, redaction, or other methods and was, or was reasonably

believed to have been, acquired by an unauthorized person, creating a material risk of harm, SRP had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by S.C. Code Ann. § 39-1-90(A).

265. By failing to disclose the Data Breach in a timely and accurate manner, SRP violated S.C. Code Ann. § 39-1-90(A).

266. As a direct and proximate result of SRP violations of S.C. Code Ann. § 391-90(A), Plaintiffs and Class Members suffered damages, as described above.

267. Plaintiffs, on behalf of themselves and the South Carolina Subclass, seek relief under S.C. Code Ann. § 39-1-90(G), including actual damages and injunctive relief.

COUNT V
BREACH OF CONFIDENTIALITY
(On behalf of Plaintiffs and the Nationwide Class, or alternatively, the South Carolina Subclass and Georgia Subclass)

268. Plaintiffs restate and reallege paragraphs 1-213 above and hereafter as if fully set forth herein.

269. SRP had, by virtue of the foregoing, and its bank-customer relationship, a confidential relationship with Plaintiffs and Class Members under which the former was required to protect certain confidential information of the latter.

270. Confidential information belonging to Plaintiffs and Class Members was disclosed by Defendant in breach of the duty of confidentiality owed.

271. The disclosure was made to third parties.

272. The disclosure was unconsented to by Plaintiffs and Class Members, who had an absolute right in the confidentiality of the information and a right to avoid any injury from its disclosure.

273. As a direct and proximate result of the unconsented disclosure of protected information, judgment should be granted for nominal and punitive damages, as well as for any actual injury sustained.

COUNT VI
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiffs and the Nationwide Class, or alternatively, the South Carolina Subclass and Georgia Subclass)

274. Plaintiffs restate and reallege paragraphs 1-213 above and hereafter as if fully set forth herein.

275. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became guardian of Plaintiffs and Class Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs and Class Members' PII; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store .

276. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Defendant's relationship with its customers, in particular, to keep secure their PII.

277. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discovery, investigate, and give notice of the Data Breach in a reasonable and practicable period.

278. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt or otherwise protect the integrity of the systems containing Plaintiffs and Class Members' PII.

279. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by

failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

280. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PII. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

281. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT VII
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Nationwide Class, or alternatively, the South Carolina Subclass and Georgia Subclass)

282. Plaintiffs restate and reallege paragraphs 1-213 above and hereafter as if fully set forth herein.

283. This Count is pleaded in the alternative to Count III above.

284. Plaintiffs and Class Members conferred a benefit on Defendant. Specifically, they provided Defendant with their PII, which PII has inherent value. In exchange, Plaintiffs and Class Members should have been entitled to have Defendant protect their PII with adequate data security, especially in light of their relationship.

285. Defendant knew that Plaintiffs and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendant profited from Plaintiffs' retained data and used Plaintiffs' and Class Members' PII for business purposes.

286. Defendant failed to secure Plaintiffs' and Class Members' PII and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their PII provided.

287. Defendant acquired the PII through inequitable record retention as it failed to disclose the inadequate security practices previously alleged.

288. If Plaintiffs and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to secure their PII, they would have made alternative employment choices that excluded Defendant.

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

290. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it.

291. As a direct and proximate result of SRP's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) the imminent and substantial risk of actual identity theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v)

lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remains in SRP's possession and is subject to further unauthorized disclosures so long as SRP fails to undertake appropriate and adequate measures to protect PII in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

292. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from SRP and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by SRP from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

293. Plaintiffs and Class Members may not have an adequate remedy at law against SRP, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VIII
Litigation Expenses pursuant to O.C.G.A. § 13-6-11
(On behalf of Plaintiffs Dunn, McGrier, Chase, and Whitfield and the Georgia Subclass)

294. Plaintiffs Dunn, McGrier, Chase, and Whitfield restate and reallege paragraphs 1-213 above and hereafter as if fully set forth herein.

295. Defendant through its actions alleged and described herein acted in bad faith, was stubbornly litigious, or caused Plaintiffs and the Georgia Subclass unnecessary trouble and expense with respect to the events underlying this litigation.

296. Section 5 of the FTC Act prohibits "unfair…practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Defendant for failing to implement and use reasonable measures to protect PII.

297. Defendant violated Section 5 of the FTC ACT by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII that it obtained and stored and the foreseeable consequences of a data breach.

298. Defendant also has a duty under the Georgia Constitution ("the Constitution") which contains a Right to Privacy Clause, Chapter 1, Article 1, to protect its users' PII. The Georgia Constitution states, "no person shall be deprived of life, liberty, or property except by due process of law." Moreover, the Georgia Constitution identifies certain invasions of privacy, including the Public Disclosure of Private Life which prohibits the public disclosure of private facts.

299. This duty has been recognized by the Georgia Supreme Court in the Restatement of the Law of Torts (Second) §652A which specifically recognized four common law invasion of privacy claims in Georgia, which include 1) appropriation of likeness; 2) intrusion on solitude or seclusion; 3) public disclosure of private facts; and 4) false light.

300. Defendant's implementation of inadequate data security measures, its failure to resolve vulnerabilities and deficiencies, and its abdication of its responsibility to reasonably protect data it required Plaintiffs and the Georgia Subclass to provide and store on its own servers constitutes a violation of the Georgia Constitution and the Restatement of the Law of Torts (Second).

301. Defendant knew or should have known that it had a responsibility to protect the PII it required Plaintiffs and the Georgia Subclass to provide and stored, that it was entrusted with this PII, and that it was the only entity capable of adequately protecting the PII.

302. Despite that knowledge, Defendant abdicated its duty to protect the PII it required Plaintiffs and the Georgia Subclass to provide and that it stored.

303. As a direct and proximate result of Defendant's actions, Plaintiffs' and the Georgia Subclass Members' PII was stolen. As further alleged above, the Data Breach was a direct consequence of Defendant's abrogation of data security responsibility and its decision to employ knowingly deficient data security measures that knowingly left the PII unsecured. Had Defendant adopted reasonable data security measures, it could have prevented the Data Breach.

304. As further described above, Plaintiffs and the Georgia Subclass have been injured and suffered losses directly attributable to the Data Breach.

305. Plaintiffs and the Georgia Subclass therefore request that their claim for recovery of expenses of litigation and attorneys' fees be submitted to the jury, and that the Court enter a judgment awarding their expenses of litigation and attorneys' fees pursuant to O.C.G.A. § 13-6-11.

PRAYER FOR RELIEF

Plaintiffs and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiffs and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiffs hereby demand that this matter be tried before a jury.

Dated: November 7, 2025.

Respectfully Submitted,

/s/ Paul Doolittle
Paul J. Doolittle, Esq. (S.C. Fed. ID No. 6012)
POULIN | WILLEY ANASTOPOULO, LLC
32 Ann Street
Charleston, SC 29403
Tel: 803-222-2222
Fax: 843-494-5536
Email: paul.doolittle@poulinwilley.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878

Email: gklinger@milberg.com

CHESTNUT CAMBRONNE PA
Bryan L. Bleichner*
Philip J. Krzeski*
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612) 336-2940
Email: bbleichner@chestnutcambronne.com
Email: pkrzeski@chestnutcambronne.com

Jonathan T. Deters*
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
jdeters@msdlegal.com

Attorneys for Plaintiff Allen

/s/ Karolan Ohanesian
Karolan Ohanesian (S.C. Fed ID 6056)
Glenn V. Ohanesian (S.C. Fed ID 5317)
OHANESIAN LAW FIRM
P.O. Box 2433
Myrtle Beach, SC 29578
Phone: 843-626-7193
Fax: 843-492-5164
Email: OhanesianLawFirm@cs.com

Samuel J. Strauss*
Raina Borrelli*
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, IL 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
sam@straussborrelli.com
raina@straussborrelli.com

Attorneys for Plaintiff Black

/s/ Paul Doolittle
Paul Doolittle (S.C. Fed. ID No. 6012)

POULIN | WILLEY | ANASTOPOULO, LLC
32 Ann Street
Charleston, SC 29403
T: (803) 222-2222
F: (843) 494-5536
pauld@akimlawfirm.com

N. Nickolas Jackson (pro hac vice forthcoming)
THE FINLEY FIRM, P.C.
3355 Lenox Road, N.E., Suite 750
Atlanta, GA 30326
Phone: (706) 928-9920
njackson@thefinleyfirm.com

Attorneys for Plaintiff Whitfield

/s/ Ryan P .Duffy
Ryan P. Duffy (S.C. Fed. ID No. 13520)
THE LAW OFFICE OF RYAN P. DUFFY
1213 W. Morehead St., Suite 500, Unit #450
Charlotte, NC 28208
Phone: (704) 741-9399
Email: rduffy@ryanpduffy.com

Manuel S. Hiraldo*
HIRALDO P.A.
401 E Las Olas Blvd., Suite 1400
Ft. Lauderdale, FL 33301
Phone: (954) 400-4713
Email: mhiraldo@hiraldolaw.com

Michael Eisenband
EISENBAND LAW, P.A.
515 E Las Olas Blvd., Suite 120
Ft. Lauderdale, FL 33301
Phone: (954) 732-2792
Email: meisenband@eisenbandlaw.com

Attorneys for Plaintiff Oscar Ortiz

/s/ Karolan Ohanesian
Karolan Ohanesian (S.C. Fed ID 6056)
Glenn V. Ohanesian (S.C. Fed ID 5317)
OHANESIAN LAW FIRM

P.O. Box 2433
Myrtle Beach, SC 29578
Phone: 843-626-7193
Fax: 843-492-5164
Email: OhanesianLawFirm@cs.com

Mark Svensson*
LEVI & KORSINSKY, LLP
33 Whitehall Street, 17th Floor
New York, NY 10004
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: msvensson@zlk.com

Attorneys for Plaintiff Theresa McGrier

/s/ David A. Maxfield
David A. Maxfield (S.C. Fed. ID No. 6293)
SOCO80808 Building 808 D Lady Street
Columbia, SC 29201
Tel: (803) 509-6800
Fax: (855) 299-1656
Email: dave@consumerlawsc.com

BRONSTEIN, GEWIRTZ& GROSSMAN,LLC
Michael J. Boyle, Jr. (pro hac vice to be filed)
4200 Regent Street, Suite 200
Columbus, OH 43219
Tel: (614) 578-5582
Email: mboyle@bgandg.com

Peretz Bronstein (pro hac vice to be filed)
60 East 42nd Street, Suite 4600
NewYork, NY 10165
Tel: (212) 697-6484
Fax: (212) 697-7296
Email: peretz@bgandg.com

Attorneys for Plaintiff Dunn

/s/ Paul Doolittle
Paul J. Doolittle, Esq. (S.C. Fed. ID No. 6012)
POULIN | WILLEY ANASTOPOULO, LLC
32 Ann Street
Charleston, SC 29403
Tel: 803-222-2222

Fax: 843-494-5536
Email: paul.doolittle@poulinwilley.com
cmad@poulinwilley.com

Marc H. Edelson*
EDELSON LECHTZIN LLP
411 S. State Street, Suite N300
Newtown, PA 18940
Phone: (215) 867-2399
Email: medelson@edelson-law.com

Attorneys for Plaintiff Chase