UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
AIKEN DIVISION

VINCENT CERRATO, *individually and on behalf of all others similarly situated*, Plaintiff, v. SRP FEDERAL CREDIT UNION, Defendant.	Case No. 1:24-cv-07684-CMC **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Vincent Cerrato ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against SRP Federal Credit Union ("SRPFCU"). The following allegations are based on Plaintiff's knowledge, investigations of counsel, facts of public record, and information and belief.

INTRODUCTION

1. This action seeks justice for the harm caused by SRPFCU's grossly inadequate and illegal data security protocols, which resulted in unauthorized access to and exposure of the Plaintiff's and Class Members' highly sensitive personal data. This data includes, but is not limited to, names, dates of birth, Social Security numbers and financial account ("PII"). The breach was perpetrated by unauthorized third-party threat actors between September 5, 2024, and November 4, 2024.[1] SRPFCU's data breach had severe consequences for the Plaintiff and Class Members, compromising their security and privacy.

2. SRP Federal Credit Union, established in 1960, operates as a member-owned

[1] *Maine Office of the Attorney General,* Notice of Data Breach: SRP Federal Credit Union, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/10844f64-85d5-4b49-b683-f9ba718f60a7.html.

financial institution dedicated to providing a wide range of financial products and services to individuals and families across South Carolina and Georgia. Committed to supporting its members, SRP FCU offers personalized loan and banking solutions designed to meet diverse financial needs.[2]

3. Upon information and belief, prior to and throughout the occurrence of the Data Breach, SRPFCU acquired the PII of the Plaintiff and Class Members and maintained this sensitive data negligently and/or recklessly. The Data Breach reveals SRPFCU's inadequate and unlawful management of its network, platform, and software. SRPFCU made its own customers vulnerable targets for unauthorized employees, who could potentially sell such data to cybercriminals or use it for other nefarious purposes.

4. Upon information and belief, SRPFCU was aware of the risks associated with the data breach. Therefore, SRPFCU knew that its inadequate data security measures posed a heightened risk of exfiltration, compromise, and theft.

5. Following the Data Breach, SRPFCU failed to promptly learn of the breach and notify the affected Plaintiff and Class Members of the nature and scale of the exposure, thereby exacerbating their injuries. SRPFCU's delay deprived them of the opportunity to take swift action to protect themselves and mitigate the harm. SRPFCU left the Plaintiff and Class Members uninformed, causing their injuries to worsen and the damage to proliferate.

6. Defendant issued Notice of the Data Breach Letter (the "Notice of Breach Letter") on December 12, 2024 to Plaintiff and Class.

7. Based on the Notice of Data Breach Letter, Defendant admits that Plaintiff's and Class Members' PII was unlawfully accessed and exfiltrated.

[2] https://srpfcu.org/about/ (last accessed: December 23, 2024).

8. As a result of SRPFCU's acts, Plaintiff's and the Class Members' identities are now at risk. They face an ongoing and significant threat of fraud and identity theft, necessitating constant vigilance over their financial accounts.

9. The PII accessed in the Data Breach could equip criminals to commit a wide range of financial crimes. Criminals can trade and monetize PII that SRPFCU exposed to open new financial accounts, take out loans, obtain medical services, secure government benefits, file fraudulent tax returns, obtain driver's licenses with their own photographs under Class Members' names, and provide false information to police during arrests.

10. Plaintiff and Class Members will likely incur additional financial costs for purchasing essential credit monitoring services, credit freezes, credit reports, and other protective measures to deter and detect identity theft.

11. Plaintiff and Class Members have suffered—and will continue to suffer—the loss of the benefit of their bargain, unexpected out-of-pocket expenses, diminished value of their PII, emotional distress, and the expenditure of their time in efforts to mitigate the consequences of the Data Breach

12. Through this herein action, Plaintiff seeks to remedy these injuries on behalf of himself and all similarly situated individuals whose PII was compromised in the Data Breach.

13. Plaintiff seeks remedies including, but not limited to, compensatory damages, punitive damages, reimbursement of out-of-pocket expenses, and injunctive relief. This relief includes improvements to SRPFCU's data security systems, annual audits, and the appointment of an independent, qualified cyber auditor to monitor SRPFCU's cyber vigilance, all funded by SRPFCU.

PARTIES

14. Plaintiff Vincent Cerrato is a natural person and resident and citizen of Williston,

Georgia, customer at SRPFCU from 2022 through present. On or about December 12, 2024, Cerrato received a letter informing her of the Data Breach ("Data Breach Notification"), as described more fully below.

15. Defendant SRP Federal Credit Union is a corporation organized under the laws of South Carolina, and its headquarters and principal place of business are located at 1070 Edgefield Road North, Augusta, South Carolina, 29860.

JURISDICTION AND VENUE

16. 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. The number of class members exceeds 100, many of whom have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

17. This Court has personal jurisdiction over Defendant because it operates and are headquartered in this District and conduct substantial business in this District.

18. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is based in this District, maintains Plaintiff's and Class Members' PII in this District, and has caused harm to Plaintiff and Class Members in this District.

FACTUAL ALLEGATIONS

SRPFCU's Business

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

20. SRPFCU received and maintained personally PII of its customers, including individuals' names, addresses, dates of birth, and Social Security numbers, and other financial and bank transactions. These records are stored on SRPFCU's internal systems.

21. SRPFCU promises to implement reasonable measures to safeguard the sensitive PII that it collects from theft and misuse.

22. SRPFCU acquired, collected, stored, and represented that it maintained reasonable security measures over the Plaintiff's and Class Members' PII.

23. By obtaining, collecting, receiving, and storing the Plaintiff's and Class Members' PII, SRPFCU assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting this information from unauthorized disclosure.

24. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. These measures include protecting their usernames and passwords, using strong passwords for their accounts, and avoiding potentially unsafe websites.

25. Plaintiff and the Class Members relied on SRPFCU to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

26. SRPFCU could have prevented or mitigated the effects of the data breach by securing its network more effectively, properly encrypting its data, and regulating and logging access to client PII.

27. The increasing frequency and sophistication of data breach attacks in recent years has underscored these warnings. Yet, despite these clear indications of heightened risk, SRPFCU failed to implement adequate security measures to protect against such threats.

28. SRPFCU failed to take appropriate steps to protect the Plaintiff's and Class Members' PII from being compromised. These failures include: (i) not properly selecting its

information security partners, (ii) failing to ensure the proper monitoring and logging of employee access to PII, (iii) failing to ensure the proper monitoring and logging of file access and modifications, (iv) not properly training its own and its technology partners' employees in cybersecurity best practices, (v) failing to implement fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Plaintiff and Class Members, (vi) not timely and accurately disclosing that the Plaintiff's and Class Members' PII had been improperly acquired or accessed.

29. Despite obvious risks, SRPFCU knowingly disregarded standard information security principles by allowing unmonitored and unrestricted access to unsecured PII. This disregard for basic security protocols significantly heightened the vulnerability of the data, leaving it exposed to potential breaches and exploitation.

30. Despite the known risk and foreseeable likelihood of breach and misuse, SRPFCU neglected to offer adequate supervision and oversight of the PII entrusted to it.

31. SRPFCU neglected to monitor user access to the sensitive PII disclosed in the Data Breach and failed to supervise user activity to identify potential threats.

32. SRPFCU has both past and ongoing obligations established by reasonable industry standards, common law, state statutory law, and its own assurances and representations. These obligations entail maintaining the confidentiality of the Plaintiff's and Class Members' PII and safeguarding it against unauthorized access.

33. Yet SRPFCU failed to ensure the proper implementation of sufficient processes to promptly detect and respond to data breaches, security incidents, or intrusions, such as the unauthorized access that occurred in this case.

The Data Breach

34. On November 22, 2024, Defendant learned that an unauthorized person was making

data available that was allegedly taken from a SRPFCU database.

35. Further investigation determined that and unknown and unauthorized third party accessed Defendant's computer systems sometime between September 5, 2024, and November 4, 2024.

36. Based on the Notice of Data Breach Letter, Defendant admits that Plaintiff's and Class Members' PII was unlawfully accessed and exfiltrated.

37. SRPFCU unreasonably delayed several weeks before notifying Plaintiff and the Class Members that their PII had been exposed.

38. Time is crucial when highly sensitive PII is subjected to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired the PII of the Plaintiff and Class Members may now be available on the Dark Web, for sale to criminals. As a result, the Plaintiff and Class Members are currently and continuously exposed to the risk of fraud, identity theft, and misuse stemming from the potential publication of their PII.

39. SRPFCU's offer also fails utterly to compensate Plaintiff and the Class Members for their time spent protecting themselves from SRPFCU's failures, even though SRPFCU's notice purports to put the burden of identity protection on Plaintiff and the Class Members. Time is a compensable and valuable resource in the United States, and American adults have only 36 to 40 hours of "leisure time" outside of work per week. Usually, this time can be spent at the option of the consumer, but Plaintiff and the Class Members now must spend their leisure time self-monitoring accounts, communicating with financial institutions and credit reporting agencies, contacting government agencies, researching identity protection measures, and implementing self-protection measures that SRPFCU did not offer.

40. Plaintiff and the Class Members thus seek remuneration for the loss of their valuable

time. SRPFCU, not Plaintiff and the Class Members, should pay to clean up its mess. Yet SRPFCU did not even acknowledge, much less offer to compensate Plaintiff and the Class Members for, their lost time.

41. The PII and financial information of the Plaintiff and Class Members are at risk of being sold on the dark web or exploited by companies for targeted marketing without their consent. In either scenario, unauthorized individuals can readily access the detailed PII and financial information of the Plaintiff and Class Members.

SRPFCU Fails to Comply with FTC Guidelines

42. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[3] To that end, the FTC has issued numerous guidelines identifying best data security practices that SRPFCU should have employed to protect against unauthorized access to customer Sensitive Information.

43. In 2016, the FTC revised its publication, "Protecting Personal Information: A Guide for Business, Lessons Learned From FTC Cases," outlining crucial data security principles and practices. These guidelines specify that businesses are expected to:

- protect the personal customer information that they keep;
- properly dispose of personal information that is no longer needed;
- encrypt information stored on computer networks;
- understand their network's vulnerabilities; and
- implement policies to correct security problems.[4]

[3] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed May 22, 2024).

[4] *Protecting Personal Information: A Guide for Business*, *Lessons Learned From FTC Cases*, FED. TRADE COMM'N (Oct. 2016), https://bit.ly/3u9mzre (last accessed May 22, 2024); *See Start With Security, A Guide for Business*, FED. TRADE COMMISSION,

44. The FTC has also underscored the critical importance of implementing robust data security measures through a series of comprehensive guidelines for businesses. Emphasizing the integration of data security into all facets of business decision-making, the FTC advocates for a multi-faceted approach, which includes:

- Encryption of information stored on computer networks.
- Prudent retention of payment card information for only the necessary duration.
- Proper disposal of personal information that is no longer required.
- Restriction of administrative access to business systems.
- Adoption of industry-proven methods for data security.
- Vigilant monitoring of network activity to detect unauthorized actions.
- Verification of the functionality of privacy and security features.
- Regular testing for common vulnerabilities.

45. Prompt updating and patching of third-party software.[5] The FTC advises companies to refrain from retaining PII beyond the necessary period for transaction authorization, restrict access to sensitive data, enforce the use of complex passwords for network access, employ industry-standard security measures, actively monitor networks for suspicious activity, and ensure that third-party service providers have implemented adequate security measures.[6]

46. Failure to implement of reasonable and appropriate measures to prevent unauthorized access to confidential consumer data is an unfair practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Accordingly, the FTC has initiated

---

https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Dec. 23, 2024).

[5] Federal Trade Commission, Start with Security: A Guide for Business (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Dec. 23, 2024).

[6] *Id.*

enforcement actions against businesses that have failed to sufficiently safeguard customer data. Orders resulting from these actions provide additional clarity on the specific steps that businesses must undertake to fulfill their data security responsibilities.

47. SRPFCU's failure to implement reasonable and suitable measures to safeguard against unauthorized access to PII is an unfair practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

SRPFCU's Deviation from Industry Standards

48. Entrusted with the responsibility of managing highly sensitive PII, encompassing financial and insurance details, SRPFCU possessed or should have possessed an acute awareness of the imperative to safeguard such data. Moreover, SRPFCU should have been cognizant of the foreseeable repercussions of a breach in its data security systems, including the substantial costs that would be incurred by its customers. Despite this awareness, SRPFCU neglected to implement sufficient cybersecurity measures to avert the occurrence of the Data Breach.

49. Further, SRPFCU's negligent delay in appropriately and promptly notifying the Plaintiff and Members of the Class about the Data Breach worsened the injuries suffered by both the Plaintiff and the Members of the Class. This delay deprived them of the earliest opportunity to undertake necessary actions to safeguard their PII and implement crucial measures to mitigate the adverse effects of the Data Breach. Contrary to its promises to safeguard sensitive data, SRPFCU does not adhere to industry-standard practices in securing PII.

50. Cybersecurity experts frequently highlight financial service providers as especially susceptible to data breaches due to the significant value of the PII they collect and retain.

51. Financial service providers like SRPFCU should, at a minimum, implement several industry-standard best practices. These include: educating all employees; employing strong passwords; utilizing multi-layer security, such as firewalls, anti-virus, and anti-malware software;

employing encryption to render data unreadable without a key; implementing multi-factor authentication; backing up data; and crucially, as evident in the present case, restricting access to sensitive data to authorized employees only.

52. Additional best cybersecurity practices standard in the financial service industry encompass installing suitable malware detection software; monitoring and restricting network ports; safeguarding web browsers and email management systems; configuring network systems like firewalls, switches, and routers; overseeing and securing physical security systems; fortifying against potential communication system vulnerabilities; and conducting comprehensive staff training on critical security protocols.

53. SRPFCU failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1, and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

54. These frameworks represent the established industry norms within the financial service sector. SRPFCU's failure to adhere to these widely accepted standards caused the Data Breach and has provided an avenue for criminal exploitation.

The Experiences of Plaintiff and Class Members

55. Plaintiff and the Class Members are either SRPFCU employees or customers. To receive banking services or meet employment requirements at SRPFCU, they were required to provide their PII.

56. Plaintiff and the Class Members had to divulge their PII to SRPFCU in order to receive banking services or as a condition of employment at SRPFCU.

57. SRPFCU's Data Breach caused significant harm to both Plaintiff and the Class. Despite this, SRPFCU has made minimal efforts to offer relief to the Plaintiff and the class

members for the damages they have endured.

58. All Class Members suffered harm when SRPFCU allowed unauthorized cybercriminal to exfiltrate customer and employee PII.

59. Plaintiff and the Class Members entrusted their PII to SRPFCU with the reasonable expectation that SRPFCU would, at a minimum, implement industry-standard precautions to protect, maintain, and safeguard their information from unauthorized access or disclosure, and promptly notify them of any data security incidents. Had Plaintiff and the Class members known that SRPFCU would fail to take reasonable steps to safeguard their information from unauthorized access by its employees, they would not have entrusted their PII to the SRPFCU.

60. Plaintiff and Class Members suffered actual injury due to the compromise of their PII in the Data Breach, including, but not limited to: (a) damage to and diminution in the value of their PII—a form of property obtained by SRPFCU from the Plaintiff; (b) violation of their privacy rights; (c) the probable theft of their PII; (d) probable fraudulent activity resulting from the Data Breach; and € ongoing injury arising from the heightened risk of additional identity theft and fraud.

61. As a result of the Data Breach, the Plaintiff and Class Members have expended—and will continue to expend—significant time and money to mitigate and address the harms caused by the breach.

Plaintiff and Class Face Significant Ongoing Risk of Identity Theft

62. The consequences of SRPFCU's failure to secure the Plaintiff's and Class Members' PII are severe. Identity theft involves the unauthorized use of another's personal and financial information—such as name, account number, Social Security number, driver's license number, date of birth, and other details—to commit fraud or other crimes.

63. Experts indicate that one in four individuals who receive a data breach

notification will become a victim of identity fraud.[7] This statistic underscores the significant risk and potential harm faced by those affected by a data breach, highlighting the critical importance of safeguarding personal information to prevent such widespread and damaging consequences.

64. Due to SRPFCU's failure to prevent and promptly detect the Data Breach, Plaintiff and the Class Members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have already experienced or are at an increased risk of experiencing, *inter alia*, a) Loss of control over how their PII is used; b) Diminution in the value of their PII; c) Compromise and ongoing exposure of their PII; d) Out-of-pocket expenses for the prevention, detection, recovery, and remediation of identity theft or fraud; e) Lost opportunity costs and lost wages associated with the time and effort spent addressing and attempting to mitigate the actual and future consequences of the Data Breach, including efforts to research how to prevent, detect, contest, and recover from identity theft and fraud; f) Delays in receiving tax refunds; g) Unauthorized use of their PII; and h) Continued risk to their PII, which remains in SRPFCU's possession and is vulnerable to further breaches as long as SRPFCU fails to implement appropriate protective measures.

65. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII is traded on the black market for years, with criminals often posting stolen private information openly on various "dark web" websites. This information is made publicly available for a substantial fee.[8]

66. Consequently, victims may take years to detect PII theft, allowing criminals ample time to exploit that information for financial gain.

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

[7] https://usa.kaspersky.com/blog/data-breach-letters-affected-by-identity-theft/1262/ (last visited Dec. 23, 2024).
[8] https://www.reflectiz.com/blog/pii-black-market/ (last visited Dec. 23, 2024).

packages.[9]

68. Cyber-criminals have the ability to cross-reference two sources of PII, combining unregulated data available elsewhere with criminally stolen data to create remarkably comprehensive and accurate profiles of individuals. These profiles, often referred to as "Fullz" packages, contain detailed dossiers on individuals.

69. In addition to facing substantial out-of-pocket expenses, often totaling thousands of dollars, and enduring the emotional toll of identity theft, victims frequently find themselves investing significant time in rectifying the aftermath. Those targeted by new account identity theft are typically burdened with the arduous task of rectifying fraudulent entries in their credit reports, perpetually monitoring these reports for further inaccuracies, closing existing bank or credit accounts, opening new ones, and engaging in the protracted process of disputing illegitimate charges with creditors.

70. In order to protect themselves, Plaintiff and the Class Members will need to remain vigilant against unauthorized data use for years or even decades to come.

CLASS ACTION ALLEGATIONS

71. Pursuant to Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5), Plaintiff proposes the following Class definition, subject to amendment as appropriate:

[9] "Fullz" is fraudster-speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, "Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm," KREBS ON SECURITY, (Sep. 18, 2014) https://krebsonsecurity.com/tag/fullz/ (last visited on Dec. 23, 2024).

72. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> **All individuals whose PII was accessed or potentially compromised during the data breach referenced in the Notice of Data Breach issued by the Defendant to the Plaintiff and other Class Members on or about December 12, 2024 (the 'Class').**

73. The Class defined above is readily ascertainable from information in SRPFCU's possession. Thus, such identification of Class Members will be reliable and administratively feasible.

74. Excluded from the Class are: (1) any judge or magistrate presiding over this action and members of their families; (2) SRPFCU, its' subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which SRPFCU or its parent has a controlling interest, and its current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and SRPFCU's counsel; (6) members of the jury; and (7) the legal representatives, successors, and assigns of any such excluded persons.

75. Plaintiff reserves the right to amend or modify the Class definition—including potential Subclasses—as this case progresses.

76. Plaintiff and Class Members satisfy the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

77. **Numerosity**. The Class Members are numerous such that joinder is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of hundreds of thousands of individuals who reside in the U.S. and were customers of SRPFCU and whose PII was compromised by the Data Breach.

78. **Commonality**. There are many questions of law and fact common to the Class.

And these common questions predominate over any individualized questions of individual Class Members. These common questions of law and fact include, without limitation:

a. Whether SRPFCU unlawfully used, maintained, lost, or disclosed the Plaintiff's and Class Members' PII;

b. Whether SRPFCU failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach;

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

d. Whether SRPFCU's data security systems prior to and during the data breach were consistent with industry standards;

e. Whether SRPFCU owed a duty to Class Members to safeguard their PII;

f. Whether SRPFCU breached its duty to Class Members to safeguard their PII;

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

h. Whether SRPFCU took reasonable measures to assess the extent of the data breach after its discovery;

i. Whether SRPFCU failed to provide notice of the Data Breach in a timely manner;

j. Whether SRPFCU's delay in informing Plaintiff and Class Members of the Data Breach was unreasonable;

k. Whether SRPFCU's conduct was negligent;

l. Whether SRPFCU and Class Members were injured as a proximate cause or result of the Data Breach;

m. Whether SRPFCU and Class Members suffered legally cognizable damages

as a result of SRPFCU's misconduct;

n. Whether SRPFCU breached express or implied contracts with Plaintiff and Class Members;

o. Whether SRPFCU was unjustly enriched as a result of the Data Breach; and

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

79. **Typicality**. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach. Moreover, Plaintiff and all Class Members were subjected to SRPFCU's uniformly illegal and impermissible conduct.

80. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating complex class actions. Plaintiff has no interests that conflict with, or are antagonistic to, those of the Class.

81. **Predominance**. SRPFCU has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff and Class Members' data was stored on the same network system and unlawfully and inadequately protected in the same way. The common issues arising from SRPFCU'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.

82. **Superiority**. A class action offers a superior means for the fair and efficient resolution of the controversy at hand. By consolidating common questions of law and fact, class treatment surpasses the alternative of pursuing multiple individual actions or fragmented litigation. Without the option of a class action, the majority of Class Members would likely discover that the

cost associated with litigating their individual claims is prohibitively high, rendering them without an effective remedy. Moreover, prosecuting separate actions by individual Class Members would introduce the risk of inconsistent or divergent adjudications, thereby establishing incompatible standards of conduct for SRPFCU. In contrast, managing this matter as a class action poses fewer logistical challenges, preserves judicial resources, conserves the parties' resources, and safeguards the rights of each Class Member.

83. The litigation of the claims presented here is manageable. SRPFCU's uniform conduct, the consistent application of relevant laws, and the easily ascertainable identities of Class Members indicate that prosecuting this lawsuit as a class action would not present significant manageability problems.

84. Adequate notice can be given to Class Members directly using information maintained in SRPFCU's records.

85. Similarly, certain issues falling under Rule 23(c)(4) warrant certification, as these claims involve specific common issues pivotal to advancing the resolution of this matter and serving the interests of all parties involved.

86. SRPFCU's actions have implications that extend uniformly across the entire Class, thus justifying Class certification, as well as the pursuit of injunctive and corresponding declaratory relief on a comprehensive, Class-wide basis.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

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

88. SRPFCU required its customers to submit the non-public PII of the Plaintiff and Class Members to receive SRPFCU's banking and financial services.

89. By collecting, storing, sharing, and using this data for commercial gain, SRPFCU owed a duty of care to use reasonable means to secure and safeguard its computer systems, including the Plaintiff's and Class Members' PII. This duty included preventing unauthorized access and promptly detecting and notifying affected individuals in the event of a data breach.

90. SRPFCU could foresee that unauthorized individuals would attempt to access and misuse the PII. Given the vast amounts of PII held by SRPFCU, it was inevitable that unauthorized individuals, including its own employees, would at some point attempt to access its PII databases.

91. Given the high value of PII, SRPFCU knew or should have known the risks involved in obtaining, using, handling, emailing, and storing the PII of the Plaintiff and Class Members. Therefore, SRPFCU was aware, or should have been aware, of the importance of exercising reasonable care in handling the PII entrusted to them.

92. SRPFCU owed a duty of care to the Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein. This included ensuring that its systems, networks, service providers, and responsible personnel adequately protected the PII.

93. SRPFCU's duty to use reasonable security measures to restrict unauthorized access arose from the special relationship between SRPFCU and the Plaintiff and Class Members, as recognized by laws, regulations, and common law. SRPFCU was in a superior position to ensure that its own systems, and those of its service providers, were adequate to protect against the foreseeable risk of harm from a data breach.

94. SRPFCU's duty to implement reasonable security measures also arises under the FTCA. This statute prohibits "unfair practices in or affecting commerce," which, as interpreted and enforced by the FTC, includes the failure to use reasonable measures to protect confidential data.

95. Furthermore, the injuries sustained by the Plaintiff and Class Members are precisely the type of injuries protected against by the FTCA. The FTC has pursued numerous enforcement actions against businesses that, due to their failure to implement reasonable data security measures and avoid unfair and deceptive practices, caused the same injuries suffered by the Plaintiff and Class Members due to SRPFCU 's actions.

96. SRPFCU's failure to comply with FTCA and other statutory duties and standards of conduct constitutes negligence.

97. SRPFCU's obligation to exercise reasonable care in safeguarding confidential data also arises from industry standards mandating the protection of confidential PII.

98. SRPFCU's failure to comply with the requisite standard of care caused the Breach, exposing Plaintiff's and Class Members' PII to cybercriminals and causing Plaintiff and Class Members pecuniary and non-pecuniary harm detailed herein.

99. SRPFCU also owed Plaintiff and Class Members a duty to promptly notify them of any breach to their PII within a reasonable timeframe. Additionally, SRPFCU was obligated to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. This duty is essential for Plaintiff and Class Members to take appropriate measures to protect their PII, remain vigilant in the face of increased risk, and undertake necessary steps to mitigate the consequences of the Data Breach.

100. SRPFCU owed these duties to Plaintiff and Class Members because they belong to a clearly identifiable and foreseeable group of individuals who SRPFCU knew or should have known would suffer actual harm due to its inadequate security protocols. Moreover, SRPFCU actively sought and obtained the PII of Plaintiff and Class Members, further underscoring its responsibility to safeguard their information.

101. SRPFCU breached its duties, and thus was negligent, by failing to use reasonable

measures to protect Plaintiff's and Class Members' PII. The specific negligent acts and omissions committed by SRPFCU include, but are not limited to:

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

b. Failing to comply with—and thus violating—FTCA and its respective regulations;

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

d. Failing to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' PII;

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

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

102. SRPFCU's failure to implement reasonable measures to protect Class Members' PII made it foreseeable that Class Members would suffer injury. Moreover, given the frequent occurrence of cyberattacks and data breaches in the financial service industry, the breach of security was reasonably foreseeable. Therefore, it was foreseeable that the inadequate safeguarding of Class Members' PII would lead to various types of injuries.

103. The injury and harm suffered by the Plaintiff and Class Members were the reasonably foreseeable results of SRPFCU's failure to exercise reasonable care in safeguarding and protecting their PII. SRPFCU knew or should have known that its systems and technologies for processing and securing the Plaintiff's and Class Members' PII had security vulnerabilities.

104. As a result of SRPFCU's negligence, the PII and other sensitive information of the

Plaintiff and Class Members were compromised, placing them at a greater risk of identity theft and unauthorized disclosure to third parties without their consent.

105. In sum, SRPFCU's negligence directly and proximately caused the Plaintiff and Class Members to suffer actual, tangible injuries and damages. These injuries include, but are not limited to, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, diminished value of their PII, and the time and money spent to mitigate and remediate the effects of the data breach. Additionally, these injuries and damages are ongoing, imminent, and immediate.

106. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

107. In addition to monetary relief, the Plaintiff and Class Members are entitled to injunctive relief requiring SRPFCU to strengthen its data security systems and monitoring procedures, conduct periodic audits of these systems, and provide credit monitoring and identity theft insurance to the Plaintiff and Class Members for a period of ten years.

COUNT II
Breach of Third-Party Beneficiary Contract
(On Behalf of the Plaintiff and the Class)

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

109. SRPFCU executed written contracts with its customers to provide banking and financial services.

110. These contracts included promises by SRPFCU to secure, safeguard, and not disclose Plaintiff's and Class Members' PII.

111. These contracts were expressly crafted for the benefit of the Plaintiff and Class Members, serving as intended third-party beneficiaries of the agreements established between

SRPFCU and its clients. SRPFCU was aware that any breach of these contracts with its clients would result in harm to the employees of said clients—the Plaintiffs and Class Members.

112. SRPFCU's clients fully performed their obligations under their contracts with SRPFCU.

113. Yet, despite this obligation, SRPFCU failed to secure, safeguard, and/or maintain the privacy of the Plaintiff's and Class Members' PII. SRPFCU permitted unauthorized employees to access the Plaintiff's and Class Members' PII without permission. Consequently, SRPFCU breached its contracts with the Plaintiff and Class Members.

114. As a consequence of the breach of contracts between SRPFCU and its clients, the Plaintiff and Class Members have suffered harm, damage, and/or injury as outlined in this document.

115. Plaintiff and Class Members, as third-party beneficiaries of the contracts between SRPFCU and its clients, are entitled to compensatory, consequential and nominal damages suffered as a result of the Data Breach.

116. In addition to monetary relief, the Plaintiff and Class Members are entitled to injunctive relief requiring SRPFCU to strengthen its data security systems and monitoring procedures, conduct periodic audits of these systems, and provide credit monitoring and identity theft insurance to the Plaintiff and Class Members for a period of ten years.

COUNT III
In the Alternative—Breach of Implied Contract
(On Behalf of the Plaintiff and the Class)

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

118. The Plaintiff brings this count as an alternative to the breach of a third-party contract claim (Count II) above.

119. Plaintiff and Class Members were obligated to provide their PII to SRPFCU as part of the process of acquiring financial services from the company.

120. SRPFCU actively solicited, offered, and encouraged Class Members to provide their PII as part of its regular business practices. Plaintiff and Class Members accepted SRPFCU's invitations and willingly provided their PII to the company.

121. SRPFCU accepted possession of the Plaintiff's and Class Members' PII, ostensibly for the purpose of contracting with them.

122. Plaintiff and Class Members entrusted their PII to SRPFCU. In doing so, Plaintiff and the Class implicitly entered into contracts with SRPFCU, wherein the company agreed to safeguard and protect such information, maintain its security and confidentiality, and promptly and accurately inform Plaintiff and Class Members in case of any breach, compromise, or theft of their data.

123. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that SRPFCU's data security practices complied with relevant laws and regulations (including FTC guidelines on data security) and were consistent with industry standards.

124. Implicit in the agreement between Plaintiff and Class Members and SRPFCU to provide PII was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized access to or disclosure of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or use, (f) retain the PII only under conditions that kept such information secure and confidential.

125. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and SRPFCU on the other, is demonstrated by their conduct and course of dealing.

126. SRPFCU assured Plaintiff and the Class Members that it would safeguard their PII in a reasonably secure manner.

127. Plaintiff and the Class Members entrusted funds to the SRPFCU with the reasonable belief and expectation that SRPFCU would allocate a portion of its earnings toward ensuring adequate data security. However, SRPFCU failed to fulfill this obligation.

128. Plaintiff and the Class Members would not have entrusted their PII to SRPFCU in the absence of the implied contract between them and SRPFCU to keep their information reasonably secure.

129. Plaintiff and the Class Members would not have entrusted their PII to SRPFCU in the absence of its implied promise to monitor its computer systems and networks to ensure that they adopted reasonable data security measures.

130. Plaintiff and the Class Members fulfilled their obligations under the implied contracts with SRPFCU. SRPFCU breached its obligations under these implied contracts by neglecting to safeguard Plaintiff's and the Class Members' PII and by failing to provide accurate notice to them regarding the compromise of personal information due to the Data Breach.

131. As a direct and proximate consequence of SRPFCU's breach of the implied contracts, Plaintiff and the Class Members have suffered damages, including but not limited to: (i) the theft of their Personally Identifiable Information (PII); (ii) the loss or reduction in value of their PII; (iii) uncompensated time and opportunity costs incurred in mitigating the actual consequences of the Data Breach; (iv) loss of the benefits outlined in the original agreement; (v) opportunity costs related to efforts to mitigate the consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (viii) the persistent and likely heightened risk to their PII, which (a) remains unencrypted and susceptible to unauthorized access and misuse by third parties; and (b) remains backed up in SRPFCU's possession, subject to further unauthorized disclosures until the SRPFCU

implements appropriate and sufficient measures to safeguard the PII.

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

133. Plaintiff and Class Members are additionally entitled to injunctive relief mandating that the SRPFCU, for example, (i) enhance its data security systems and monitoring protocols; (ii) undergo annual audits of said systems and protocols in the future; and (iii) promptly furnish comprehensive credit monitoring services to all Class Members for the duration of their lives.

COUNT IV
In the Alternative—Unjust Enrichment
(On Behalf of the Plaintiff and the Class)

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

135. The Plaintiff brings this count as an alternative to the breach of a third-party contract claim (Count II) and breach of implied contract (Count III) above.

136. SRPFCU knew that Plaintiff and Class Members conferred a benefit which SRPFCU accepted. SRPFCU profited from these transactions.

137. In particular, SRPFCU enriched itself by avoiding the costs it reasonably should have invested in data security measures to protect Plaintiff's and Class Members' PII, including measures to monitor and restrict unauthorized employee access to such information. Rather than implementing a reasonable level of security that could have prevented the Data Breach, SRPFCU opted to prioritize its own profits by employing cheaper, ineffective security measures. Consequently, Plaintiff and Class Members suffered directly and proximately due to SRPFCU's decision to prioritize its profits over the necessary security measures.

138. Under the principles of equity and good conscience, SRPFCU should not be permitted to retain the money belonging to Plaintiff and Class Members, because SRPFCU failed to

implement appropriate data management and security measures that are mandated by industry standards.

139. SRPFCU failed to secure Plaintiff's and Class Members' PII, and prevent unauthorized employee access to it, and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

140. SRPFCU acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

141. If Plaintiff and Class Members knew that SRPFCU had not reasonably secured their PII, they would not have agreed to provide their PII to SRPFCU.

142. Plaintiff and Class Members have no adequate remedy at law.

143. As a direct and proximate consequence of the SRPFCU's actions, Plaintiff and Class Members have endured and will continue to endure various forms of harm, including but not limited to: (a) actual instances of identity theft; (b) the loss of control over the use of their Personally Identifiable Information (PII); (c) the compromise, publication, and/or theft of their PII; (d) expenses incurred out-of-pocket for the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (e) opportunity costs resulting from expended efforts and decreased productivity in addressing and attempting to mitigate both present and future consequences of the Data Breach, encompassing research on how to prevent, detect, contest, and recover from identity theft; (f) the ongoing risk to their PII, which remains in the possession of SRPFCU and is susceptible to further unauthorized disclosures until appropriate and sufficient measures are implemented to safeguard it; and (g) prospective expenditures of time, effort, and finances that will be necessary to prevent, detect, contest, and rectify the repercussions of the compromised PII resulting from the Data Breach throughout the lifetimes of Plaintiff and Class Members.

144. As a direct and proximate result of SRPFCU's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

145. Therefore, SRPFCU should be compelled to disgorge proceeds unjustly received from Plaintiff and Class Members into a common fund or constructive trust for their benefit. Alternatively, the SRPFCU should be required to refund the amounts that Plaintiff and Class Members overpaid for its services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class Members, requests judgment against SRPFCU and that the Court grants the following:

A. An Order certifying this action as a class action and appointing Plaintiff as Class representatives, and the undersigned as Class Counsel;

B. A mandatory injunction directing SRPFCU to adequately safeguard the PII of Plaintiff and the Class hereinafter by implementing improved security procedures and measures, including but not limited to an Order:

i. prohibiting SRPFCU from engaging in the wrongful and unlawful acts described herein;

ii. requiring SRPFCU to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring SRPFCU to delete and purge the PII of Plaintiff and Class Members unless SRPFCU can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring SRPFCU to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and

integrity of Plaintiff's and Class Members' PII;

v. requiring SRPFCU to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;

vi. requiring SRPFCU to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with SRPFCU's policies, programs, and systems for protecting PII;

vii. requiring SRPFCU to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor SRPFCU's networks for internal and external threats, including unauthorized employee access, and assess whether monitoring tools are properly configured, tested, and updated; and

viii. requiring SRPFCU to meaningfully educate all Class Members about the threats that they face because of unauthorized employee access to their PII, as well as the steps affected individuals must take to protect themselves.

C. A mandatory injunction requiring that SRPFCU provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of PII to unauthorized persons;

D. An Order requiring SRPFCU to purchase credit monitoring and identity theft protection services for each Class Member for ten years;

E. An injunction enjoining SRPFCU from further deceptive practices and making untrue statements about the Data Breach and the PII that was subject to unauthorized access;

F. An award of damages, including actual, nominal, consequential damages, and punitive, as allowed by law in an amount to be determined;

G. An award of attorneys' fees, costs, and litigation expenses, as allowed by law;

H. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law; and

I. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

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

Dated: December 26, 2024

Respectfully Submitted,

/s/ Paul J. Doolittle
Paul J. Doolittle, Esq.
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

-AND-

Sabita Soneji (application for *pro hac vice* admission forthcoming)
soneji@tzleagal.com
David W. Lawler (application for *pro hac vice* admission forthcoming)

dlawler@tzlegal.com
TYCKO & ZAVAREEI LLP
2000 Pennsylvania Avenue NW
Suite 1010
Washington, D.C. 20006
Telephone: (202) 973-0900
Facsimile: (202) 973-0950

Attorneys for Plaintiff and
the Proposed Classes