UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

DAVID DE MEDICIS, on behalf of himself and all others similarly situated, Plaintiff, vs. ALLY BANK and ALLY FINANCIAL INC., Defendants.	**Civil Action No.:** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff David De Medicis ("Plaintiff"), on behalf of himself and all others similarly situated, alleges as and for his Class Action Complaint, the following against Ally Bank and Ally Financial Inc., based upon his personal knowledge with respect to himself and his own acts, and upon information and belief, upon his own investigation and the investigation of his counsel, as to all other matters, as follows:

SUMMARY OF THE ACTION

1. In a June 11, 2021, data breach notification letter ("DB Letter"), Ally Bank and Ally Financial Inc. (collectively, "Ally" or "Defendants") disclosed that a programming code error associated with Ally's website inadvertently revealed Ally's customers' usernames and passwords to third parties with whom Ally had business relationships. The DB Letter then informed customers of steps to take to mitigate the increased threat of identity theft to them caused by the Ally Breach.

2. This is a class action lawsuit brought by Plaintiff on behalf of himself and all other persons harmed by Ally's unauthorized disclosure of Plaintiff's and Class members' (as

defined herein), Ally account usernames, passwords, and other private information to unnamed third parties (the "Data Breach" or "Breach").

3. Notably, the Data Breach did not result from a sophisticated attack perpetrated by cyber criminals or state sponsored hackers.

4. Here, the Data Breach was entirely Ally's doing. Ally negligently programmed its website portal to reveal, in clear unencrypted text, Plaintiff's and the Class's usernames and passwords used to access their Ally banking and investment accounts to Ally business partners.

5. It's difficult to imagine anything could be more central to data security at an online bank like Ally than protecting the very customer usernames and passwords that provide access to the entirety of customers' account information and assets.

6. Not only did Ally negligently program its website to reveal its customers' usernames and passwords, Ally also failed to adequately test or monitor the security of its website. Had Ally merely undertaken reasonable steps to test or monitor the security of its website, Ally would have immediately discovered and stopped revealing those usernames and passwords to third parties.

7. Ally's inexcusable failure to program, test and monitor its website to adequately safeguard the security of Plaintiff's and Class member's usernames and passwords persisted without correction.

8. After Ally finally discovered the Breach, Ally delayed notifying Plaintiff and Class members about the Breach for almost two months.

9. The Ally Breach has damaged Plaintiff and Class members who have had the security of their accounts compromised and are forced to commit time to carefully review records of all their financial dealings for suspicious activity and to address and mitigate the

heightened threat of identity theft and/or acts taken by fraudsters to commit identity theft against them.

10. Ally implicitly acknowledged the Breach harmed Plaintiff and the Class putting them at heightened risk of identity theft when, "as a precautionary measure to *help* safeguard" Plaintiff and the Class's information, Ally offered 24 months of credit monitoring by Equifax (emphasis added). But Equifax does not fully protect Plaintiff from identity theft, and even if it did, 24 months is by no means a sufficient duration of credit monitoring given the breadth and extent of personal and confidential information compromised in the Breach.

11. Therefore, Plaintiff, on behalf of himself and all those similarly situated, seeks the assistance of the Court to determine and award the proper amounts of damages Defendants' wrongful conduct has caused to the Plaintiff and the Class to suffer and to award such other relief that the Court deems just and proper.

PARTIES

12. Plaintiff David De Medicis is a Virginia resident and maintains checking, savings and securities accounts with defendant Ally Bank. Plaintiff received a DB Letter from Ally on or about June 11, 2021, notifying Plaintiff that, because of a "programming" error in its customer website, Ally breached the security of Plaintiff's username and password revealing that Private Information to unnamed "third parties with whom [defendants] have business relationships."

13. Defendant Ally Bank, a subsidiary of Ally Financial Inc., is a corporation organized under the laws of the state of Utah and maintains its headquarters at 200 W Civic Center Drive, Suite 201, Sandy, Utah 84070. Ally Bank is registered as a foreign corporation in the state of New York (DOS ID 3066925), maintains one of its key locations in New York, New

York and is a member of the FDIC. Ally Bank is one of the country's largest branchless online-only banks with about 2.3 million customers and retail deposits exceeding $124 billion.

14. Defendant Ally Financial Inc. is a corporation organized under Delaware law and maintains its headquarters at 500 Woodward Avenue, Floor 10, Detroit, Michigan 48226. Ally Financial common stock is traded on the New York Stock Exchange under the symbol "ALLY." Ally Financial is registered as a foreign corporation in the state of New York (DOS 3834452), and regularly does business in New York. Ally Financial is registered as a bank holding company under the Bank Holding Company Act and a Financial holding company under the Gramm-Leach-Bliley Act. Ally Financial describes itself as a leading digital financial-services company with passionate customer service and relentlessly focused on "Doing it Right" and being a trusted financial services provider to its consumer, commercial, and corporate customers.

JURISDICTION AND VENUE

15. This Court has jurisdiction over this Action pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d)(2). The amount in controversy exceeds $5,000,000, exclusive of costs and interest. At least one member of the putative Class is a citizen of a state different from that of Ally Bank and Ally Financial and therefore minimal diversity required under CAFA is present herein. There are more than 100 putative Class members.

16. This Court has personal jurisdiction over Ally Bank because it is registered as a foreign corporation in New York and regularly does business in this district. Ally Bank provides digital direct banking services and investment securities services to consumers throughout New York and, as such, has continuous and systematic contact with New York sufficient to provide it with the minimum contacts necessary to satisfy the principles of fair play and substantial justice

and requirements of New York's long arm statute. Ally Bank has further committed a tortious act within this district. Ally Bank purposefully availed itself of the law of New York.

17. This Court has personal jurisdiction over Ally Financial because it is registered as a foreign corporation in New York and regularly does business in New York. Ally Financial has continuous and systematic contact with New York sufficient to provide it with the minimum contacts necessary to satisfy the principles of fair play and substantial justice and requirements of New York's long arm statute. Ally Financial purposefully availed itself of the law of New York.

18. Venue is proper in this judicial district pursuant to 28 U.S.C. §1391(a) because Ally Bank committed a tortious act in this District and a substantial part of the events or omissions giving rise to the claim occurred in this District.

STATEMENT OF FACTS

19. Ally's Breach violated Ally's own policies, their commitment to keep Plaintiff's and the Class members' personal and private information, including usernames and passwords ("Private Information") secure, and the most basic standards and practices of data security.

20. Among Ally's stated policies are that: "For [customer] protection, only people who need your information to do their jobs have access to the personal information you provide us"[1] and that "***we never share your usernames and passwords with anyone***." (emphasis added)[2]

[1] https://www.ally.com/security/our-approach.html (last visited July 9, 2021).

[2] https://www.ally.com/security/our-approach.html (last visited July 9, 2021).

21. Ally represented that "Keeping [customer] accounts and personal information secure is a top priority for us"[3] and that "We use the latest encryption technology to help protect your information"[4] "Do It Right" is Ally's brand promise and value proposition.

22. Contrary to its policies and commitments Ally continuously revealed Plaintiff's and Class members' *unencrypted* usernames and passwords to unnamed third parties who had business relationships with the Ally. Ally then took at least two months to notify Plaintiff and the Class of the Breach, from April 12, 2021, when Ally claims to have first discovered its programming error to June 11, 2021, when DB Letters were sent to Plaintiff and other Class members.

23. Ally failed to exercise the proper duty of care to secure its customers' Private Information including, among other things, its failure to encrypt usernames and passwords, and its sharing of usernames and passwords to persons who did not need such private information to do their jobs.

24. Ally's DB Letter states that during an update to the Company's website, "a programming code error occurred that inadvertently resulted in your username and password being exposed to third parties with whom we have business relationships" . . . "Upon detecting the error on April 12, 2021, we immediately updated the programming code to ensure it no longer included username and password information."

25. The DB Letter, however, omits to disclose, among other things:

a. how long Ally's programming error that revealed customers' usernames and passwords to third parties went undetected by Ally;

[3] https://www.ally.com/security/ (last visited July 9, 2021).

[4] https://www.ally.com/security/our-approach.html (last visited July 9, 2021).

b. the number of third parties the programming error revealed usernames and passwords;

c. the identities of third parties the programming error revealed usernames and passwords;

d. that the programming error revealed usernames and passwords to the third parties in unencrypted clear text;

e. how the third parties used or monetized information about Ally Bank customers accessed via the Ally website, including usernames and passwords;

f. whether any third parties stored Plaintiff's and Class members' Ally Bank usernames and passwords on computer systems outside of Ally's control;

g. whether any third parties continue to have access to Plaintiff's and Class members' Ally Bank usernames and passwords or other Private Information; and

h. whether any third parties, intentionally or unintentionally, disclosed Plaintiff's and Class members' private information from the Ally website to others.

26. Ally's extended, company-wide, and inexcusable Breach is particularly egregious given Ally's repeated admonitions that usernames and passwords be vigilantly safeguarded at all times directed at the Plaintiff and Class, including the admonitions to ***never disclose passwords, usernames and other personal details when money involved*** such as:

> **Protect your passwords.** Be cautious about your usernames and passwords with people, companies and services – especially when your personal information and

> money are involved. Never store your passwords in a note, memo or file on your computer or mobile device.[5]
>
> * * *
>
> Think carefully before you provide personal details on social networks like Facebook, Twitter and LinkedIn. **Never share information that financial institutions might use to identify you** like your Social Security number (including the last 4 digits), date of birth, personal phone number, home address, where you were born or schools you attended. Criminals might use this information to gain access to your account or use it to open accounts in your name (emphasis original).[6]
>
> * * *
>
> Always shred documents that contain personal information instead of placing them in your trashcan or recycling bin . . . **Criminals look for personal information in trashcans and use it to access your accounts or open new accounts** using your identity (emphasis original).[7]

27. The Ally Breach exposed precisely the types of Private Information that criminals use to commit identity theft.

28. Ally's customer usernames and passwords expose and link to the customer's name, among other things:

(a) email addresses;

(b) Account numbers;

(c) Account balances;

(d) Checking, savings and investment account statements all transactions therein;

(e) Images of all checks;

(f) Names and dates of birth of account beneficiaries;

---

[5] https://www.ally.com/security/password-security-tips.html (last visited July 11, 2021).

[6] https://www.ally.com/security/social-media-safety.html

[7] https://www.ally.com/security/how-to-protect-yourself-offline.html (last visited July 11, 2021).

(g) Employment information;

(h) Linked bank accounts including last four digits of linked bank account numbers;

(i) Tax forms with last four digits of Social Security Numbers; and

(j) Zelle account information and transaction history.

29. Ally's negligence in the programming, maintenance and monitoring of Ally's website, and utter failure to implement adequate and reasonable security measures to protect usernames and passwords and other Private Information of the Plaintiff and Class members has caused Plaintiff and the Class significant damages.

30. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by his Private Information not being properly protected.

31. Mr. De Medicis has been compelled to devote time to deal with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the DB Letter, exploring credit monitoring and identity theft protection, self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

32. Mr. De Medicis spent time changing the passwords and usernames on many of his personal online accounts.

33. Mr. De Medicis suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that Mr. De Medicis entrusted to Defendants for the purpose of facilitating his bank account and securities account, which was compromised in and because of the Data Breach.

34. Mr. De Medicis suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

35. Mr. De Medicis has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his lost Private Information, being placed in the hands of unauthorized third parties and possibly criminals.

36. Mr. De Medicis has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

37. Defendants could have prevented this Data Breach by simply programming its website properly and encrypting Plaintiff's and Class members' Private Information.

38. Defendants' negligence in safeguarding its customers' Private Information is exacerbated by the repeated warnings and alerts directed to protecting and securing electronics.

39. It is well known that Private Information is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches Ally continued to disseminate the Private Information of Plaintiff and Class members to third parties.

40. Legitimate organizations and the criminal underground alike recognize the value of Private Information contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it.

41. At all relevant times, Ally knew, or reasonably should have known, of the importance of safeguarding Private Information and of the foreseeable consequences that would occur, including, specifically, the significant costs that would be imposed on individuals as a result of a breach.

42. Unfortunately, Ally's approach to maintaining the privacy and security of the Private Information of Plaintiff and Class members was lackadaisical, cavalier, reckless, or at the very least, negligent.

43. The ramifications of Ally's failure to keep Plaintiff's and Class members' data secure are severe.

44. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[8] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[9]

45. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[10]

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[11]

---

[8] 17 C.F.R § 248.201 (2013).
[9] *Id.*

[10] Victims of Identity Theft, 2014 (November 13, 2017) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited July 30, 2021).

[11] GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited July 30, 2021).

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

48. The Private Information of Plaintiff and Class members is private and sensitive in nature and was left inadequately protected by Ally.

49. To date, Defendants have offered its customers only two years of credit monitoring through Equifax. The offered service is inadequate to protect Plaintiff and Class members from the threats they face for years to come, particularly given the Private Information at issue here.

50. The injuries to Plaintiff and Class members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for its customers.

51. Since the Ally Breach, on three separate occasions, the Plaintiff has encountered attempts by hacker to reset the password of his email account without his knowledge or permission.

CLASS ALLEGATIONS

52. Pursuant to Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiff brings this case as a class action on behalf of a Class defined as follows:

> All persons in the United States whose Private Information was compromised in the data breach announced by Ally Bank on or about June 11, 2021.

53. The Class is so numerous that joinder of all members is impracticable. On information and belief, the Class has more than one million members. Among other things, Ally Bank has 2.33 million deposit customers and 425,000 investment brokerage accounts. Moreover,

the disposition of the claims of the Class in a single action will provide substantial benefits to all parties and the Court.

54. Numerous questions of law and fact are common to Plaintiff and members of the Class. Common questions of law and fact include, but are not limited to, the following:

(a) whether Ally was negligent in programming its website such that unencrypted clear text customer usernames and passwords were revealed to third parties;

(b) how long the programing error that revealed usernames and passwords went undetected by Ally;

(c) the extent of dissemination of usernames and passwords revealed due to the website programing error;

(d) whether Ally was negligent in monitoring the operation of their website;

(e) the Private Information of Plaintiff and the Class accessible with their usernames and passwords;

(f) whether Ally failed to maintain adequate industry standard safeguards to protect the Private Information of the Plaintiff and members of the Class; and

(g) the harm Ally's conduct has caused Plaintiff and the Class to suffer.

55. Plaintiff's claims are typical of the claims of the Class's claims. Plaintiff suffered the same injury as Class members – i.e., Plaintiff's Private Information was compromised in the Breach.

56. Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has retained competent and capable attorneys with significant experience in complex and class action

litigation, including data breach class actions. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the Class and have the financial resources to do so. Neither Plaintiff nor his counsel have interests that are contrary to or that conflict with those of the proposed Class.

57. Ally's conduct at issue in this action is common to Plaintiff and other members of the Class. The common issues arising from this conduct that affect Plaintiff and members of the Class predominate over any individual issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

58. A class action is the superior method for the fair and efficient adjudication of this controversy. Class members' interests in individually controlling the prosecution of separate actions are low given the magnitude, burden, and expense of individual prosecutions against large corporations such as Ally Bank and Ally Financial. It is desirable to concentrate this litigation in this forum to avoid burdening the courts with individual lawsuits. Individualized litigation presents a potential for inconsistent or contradictory judgments, increase the delay and expense to all parties and the court system presented by the legal and factual issues of this case. By contrast, the class action procedure here will have no management difficulties. Ally's records and the records available publicly will easily identify the Class members. The same common documents and testimony will be used to prove Plaintiffs' claims. The class action procedure here will have no management difficulties.

59. A class action is appropriate under Fed. R. Civ. P. 23(b)(2) because Ally has acted or refused to act on grounds that apply generally to Class members, so that final injunctive relief or corresponding declaratory relief is appropriate as to all Class members.

COUNT I

Negligence

60. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

61. Ally required Plaintiff and members of the Class create usernames and passwords and to submit non-public financial and other Private Information to open, use and maintain deposit and securities accounts at Ally.

62. By collecting and storing this data, and using it for commercial gain, Ally had a duty of care to use reasonable means to secure and safeguard this Private Information to prevent unauthorized disclosure and to safeguard the privacy of that Private Information.

63. Ally's duties included a responsibility to implement a procedures and practices to secure Private Information from inadvertent unauthorized disclosure, to promptly detect any such unauthorized disclosure and give prompt notice to Plaintiff or any other member of the Class affected by such data breach.

64. Ally also owed a duty of care to Plaintiff and members of the Class to provide security of their Private Information consistent with industry standards and to ensure that their websites and systems, networks and the personnel responsible for them adequately protected their customers' Private Information.

65. Only Ally was in a position to program its website and to ensure that its website was safe for customers to use such that their Private Information entrusted with Ally was secure.

66. Ally breached its duty by failing to use reasonable measures to protect Plaintiff's and Class members' Private Information.

67. The specific negligent acts and omissions committed by Ally include, but are not limited to, the following:

(a) programming its website in a manner that revealed rather than safeguarded customers' Private Information;

(b) failing to adequately monitor the operation of their website;

(c) failing to timely discover the programming error; and

(d) failing to timely notify Plaintiff and members of the Class of the programming error and Breach.

68. It was foreseeable that lack of reasonable care in programming, testing and monitoring the website used by Plaintiff and members of the Class to transmit and access Private Information would result in injury to Plaintiff and other members of the Class.

69. It was also foreseeable that the lack of reasonable care in programming, testing and monitoring the website would cause injury to Plaintiff and members of the Class such as: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

70. Accordingly, Plaintiff, individually and on behalf of all those similarly situated, seeks an order declaring that Defendants' conduct alleged herein constitutes negligence and awarding damages in an amount to be determined at trial.

COUNT II

Negligence *Per Se*

71. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

72. Section 5 of the Federal Trade Commission Act, 15 U.S.C. 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice by companies such as Ally's failing to use reasonable measures to protect Private Information. Various FTC publications and orders also form the basis of Ally's duty.

73. Ally violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Private Information and not complying with industry standards.

74. Ally's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

75. Plaintiff and the members of the Class are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

76. The harm Ally caused Plaintiff and members of the Class to suffer is the type of harm the FTC Act (and similar state statutes) was intended to guard against. The FTC itself has pursued numerous enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered here.

77. As a direct and proximate result of Ally's improper conduct, Plaintiff and members of the Class have been injured and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT III

Breach of Implied Contract

78. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

79. When Plaintiff and members of the Class paid money for services Ally provided and entrusted their Private Information to Ally, they entered implied contracts with Ally pursuant to which Ally agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

80. Ally solicited and invited prospective customers to provide their Private Information through Ally's website as part of its regular business practices. These Class members accepted Ally's offers and provided their Private Information to Ally. In entering such implied contracts, Plaintiff and members of the Class assumed that Ally would "Do it Right" and undertake appropriate safeguards and data security practices and policies consistent with industry standards, and that Ally would use part of the fees paid by Plaintiff and the members of the Class to pay for adequate and reasonable data security practices.

81. Plaintiff and members of the Class would not have used the Ally's website or entrusted their Private Information with Ally in the absence of the implied contract between them and Ally to keep their usernames, passwords and other Private Information secure.

82. Plaintiff and members of the Class fully performed their obligations under the implied contract with Ally.

83. Ally breached their implied contract with Plaintiff and members of the Class by, among other things, failing to safeguard and protect their Private Information and by failing to provide timely and accurate notice that their Private Information was compromised as a result of a Data Breach.

84. As a direct and proximate result of Ally's breaches of their implied contract, Plaintiff and members of the Class sustained actual losses and damages as described in an amount to be proven at trial.

COUNT IV

Violation of the Virginia Personal Information Breach Notification Act, Va. Code. Ann. §§ 18.2-186.6, et seq.

85. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

86. Ally was required to accurately notify Plaintiff and Class members following discovery or notification of a breach of its data security system if unencrypted or unredacted Private Information was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identify theft or another fraud, without unreasonable delay under Va. Code Ann. § 18.2-186.6(B).

87. Ally owns or licenses computerized data that includes Private Information as defined by Va. Code Ann. § 18.2-186.6(B).

88. Plaintiff's and members of the Class's Private Information includes Personal Information as defined by Va. Code Ann. § 18.2-186.6(A).

89. Because Ally discovered a breach of its security system involving the Private Information of the Plaintiff and members of the Class that Ally stored, in which unencrypted or unredacted Private Information was or is reasonably believed to have been accessed and acquired

by an unauthorized person, who will, or it is reasonably believed who will, engage in identify theft or another fraud, Ally had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Va. Code Ann. § 18.2-186.6(B).

90. Ally's failure to disclose the Data Breach in a timely and accurate manner, violated Va. Code Ann. § 18.2-186.6(B).

91. As a direct and proximate result of Ally's violations of Va. Code Ann. § 18.2-186.6(B), Plaintiff and Class members suffered damages, as described above.

92. Plaintiff and Class members seek relief under Va. Code Ann. § 18.2-186.6(I), including actual damages.

COUNT V

Injunctive / Declaratory Relief, Declaratory Judgment Act, 28 U.S.C. §2201

93. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

94. The Plaintiff and members of the Class entered an implied contract that required Defendants to provide adequate security for the Private Information they collected from Plaintiff and the Class.

95. Defendants owe Plaintiff and the Class a duty of care to adequately secure their Private Information.

96. Defendants continue to possess the Plaintiff's and the Class's Private Information.

97. Other than purportedly discovering and correcting the website programming error, Defendants have announced very little in terms of changes to its security practices and infrastructure that caused the Breach to keep a similar breach from happening again.

98. There is no reason to believe that the Defendants' security practices are any more adequate now than at the time the Breach occurred.

99. Plaintiff, therefore, seeks a declaration (1) that Defendants existing data security measures do not comply with their contractual obligations and duties of care to provide adequate security of Private Information, and (2) that to comply with their obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

b. Ordering that Defendants audit, test, and train their security personnel regarding existing, new or modified security procedures;

c. Ordering Defendants to not transmit Private Information in an unencrypted form on its website;

d. Ordering the Defendants to not share Private Information with third parties without the express written permission of Plaintiff and the Class;

e. Ordering Defendants to meaningfully educate their current, former, and prospective customers about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

A. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is a proper class representative; and appoint Plaintiff's Counsel as Class Counsel;

B. That the Court grant permanent injunctive relief to prohibit Ally from engaging in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiff and members of the Class compensatory, consequential, and general damages in an amount to be determined at trial;

D. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Ally as a result of its unlawful acts, omissions, and practices;

E. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

F. That Plaintiff be granted the declaratory relief sought herein;

G. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

H. That the Court award pre- and post-judgment interest at the maximum legal rate; and

I. That the Court grant all such other relief as it deems just and proper.

Dated: August 12, 2021

Respectfully Submitted By:

KANTROWITZ, GOLDHAMER & GRAIFMAN, P.C.

Gary S. Graifman, Esq.
Melissa R. Emert, Esq.
747 Chestnut Ridge Road, Suite 200
Chestnut Ridge, NY 10977
memert@kgglaw.com
T: 845-356-2570
F: 845-356-4335

SLYNE LAW LLC
Patrick Slyne, Esq.
800 Westchester Avenue, N641
Rye Brook, NY
Patrick.Slyne@SlyneLaw.com
T: (914) 279-7000
F: (914) 653-8122

SHUB LAW FIRM LLC
Jonathan Shub, Esq.
Kevin Laukaitis*, Esq.
134 Kings Highway East, 2nd Floor
Haddonfield, NJ 08033
Tel: (610) 453-6551
Email: jshub@shublawyers.com
Email: klaukaitis@shublawyers.com

**Pro Hac Vice* Application Forthcoming

Attorneys for the Plaintiff and Members of the Putative Class