IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

Angelica LeRoy, Curtis Smith, and Loretta Smith,

Plaintiffs,

v.

SunTrust Bank, Inc.,

Defendant.

Case No.

PLAINTIFF'S CLASS ACTION COMPLAINT

Plaintiff Angelica LeRoy, Curtis Smith, and Loretta Smith (hereinafter "Plaintiffs"), individually and on behalf of the Class defined below of similarly situated persons, allege the following against SunTrust Bank, Inc. ("SunTrust") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

NATURE OF THE CASE

1. Plaintiffs bring this class action case against SunTrust for its failures to secure and safeguard its customers' personal and highly private and confidential information, including names, addresses, account balances, and other personally identifiable information ("PII") which SunTrust maintains in connection with its banking relationships with its customers, and for failing to provide timely, accurate,

and adequate notice to Plaintiffs and other Class members that their PII had been compromised.

2. SunTrust has acknowledged that approximately 1.5 million customers' PII were compromised; what is presently unknown is for what period of time this information was compromised and being taken for malicious purposes. In any event, Plaintiffs' and the Class members' PII was compromised due to SunTrust's acts, omissions, and its failure to properly protect the PII.

3. In addition to SunTrust's failure to prevent the compromise of the PII, it also failed to notify its customers when the compromise was detected in February of 2018, thereby preventing Plaintiffs and the Class members from taking action to protect themselves, and it wasn't until April 20, 2018—when SunTrust finally acknowledged the compromise—that Plaintiffs and the Class members could take any action to prevent the consequences of the compromise of their PII loss and the damages which might follow.

4. The compromise was the inevitable result of SunTrust's inadequate approach to data security and the protection of the PII that it collected during the course of its business.

5. SunTrust disregarded the rights of Plaintiffs and the Class members by intentionally, willfully, recklessly, or at the very least negligently failing to take adequate and reasonable measures to ensure the PII was protected, failing to

disclose to its customers the material fact that it did not have adequate systems and security practices in place to safeguard the PII, failing to take available steps to prevent and stop the compromise from ever happening, and failing to monitor and detect the compromise on a timely basis.

6. In addition, SunTrust exacerbated the injuries Plaintiffs and the Class members suffered by failing to provide timely notice of the compromise when SunTrust supposedly learned of the compromise in February 2018.

7. As a result of the compromise, the PII has been exposed to criminals who will obviously use the PII to the damage and to the detriment of Plaintiffs and the Class.. The injuries Plaintiffs and the Class members suffered as a direct result of SunTrust's Data Breach include:

a. theft of their personal and financial information;

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

c. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the compromise, including searching for fraudulent activity , taking the time to secure or purchasing credit monitoring and identity theft

protection services, and the stress, nuisance, and annoyance of dealing with all issues resulting from the compromise;

d. the imminent and certainly impending injury flowing from potential fraud and identify theft the compromise poses and as a result of their personal information being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class members' information on the Internet black market;

e. money paid for banking services provided by SunTrust prior to, during, and after the compromise in that Plaintiffs and the Class members would have taken steps to safeguard their PII had SunTrust disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' PII; and

f. the loss of Plaintiffs' and the Class members' privacy.

8. These injuries to Plaintiffs and the Class members were directly and proximately caused by SunTrust's failure to implement or maintain adequate data security measures for the PII and other customer data.

9. Further, Plaintiffs and the Class members retain a significant interest in ensuring that their PII and other customer data, which, while compromised, remains in the possession of SunTrust, is protected from further compromises, and

seek to remedy the harms they have suffered on behalf of themselves and similarly situated consumers whose PII and other customer data was compromised.

JURISDICTION AND VENUE

10. 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. There are more than 100 putative class members. And, at least some members of the proposed Class have a different citizenship from SunTrust.

11. This Court has personal jurisdiction over SunTrust because SunTrust maintains its principal place of business in Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia. SunTrust intentionally availed itself of this jurisdiction by marketing and selling its banking services and within Georgia.

12. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because SunTrust's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's and the Class members' claims occurred in this District.

PARTIES

13. Plaintiff Angelica LeRoy is a resident of South Carolina.

14. Plaintiffs Curtis and Loretta Smith are residents of Florida.

15. Defendant SunTrust is an American bank holding company. SunTrust Bank has subsidiaries in comprehensive financial, investment advisory, and family wealth management services; small business financing; credit card services; underwriting; affordable housing investments; re-insurance; equipment-related lease financing; mortgages; and other finance-related industries.[1] It had $205 billion in assets as of March 31, 2018.[2] SunTrust Bank's most direct corporate parent was established in 1891 in Atlanta, where its headquarters remains today.

STATEMENT OF FACTS

16. On April 20, 2018, SunTrust announced that in February, 2018, it learned that an employee accessed, for malicious reasons, highly confidential information of its customers, including their respective accounts and balances.[3] Specifically, records of some 1.5 million SunTrust customers were extracted from SunTrust's systems for purposes of sale or transfer to criminals.[4] The primary reason, of course, is obvious: for theft and damage to customers of SunTrust.

17. What SunTrust neither revealed nor sought to explain was its delay in notifying its customers of the incident. In his announcement to the public of the unauthorized and malicious intrusion, SunTrust Chairman and CEO Bill Rogers

[1] Key Subsidiaries, SunTrust Bank, Inc., https://www.suntrust.com/common/aboutst/annualreports/English/KeySub.htm (last visited May 7, 2018)
[2] SunTrust to Offer Free Identity Protection, SunTrust Bank, Inc. https://www.suntrust.com/content/dam/suntrust/us/en/internal-applications/identity-protection/document/identity-theft-release-4-20-18.pdf (last visited May 7, 2018)
[3] SunTrust Announces Possible Breach of 1.5 Million Customer Records, Theo Thimou Clark, https://www.wsbradio.com/business/personal-finance/what-know-about-the-alleged-suntrust-data-breach/HIwo9WVAHNm4G0g4mHIXLI/ (last visited May 7, 2018)
[4] *Id.*

said "[w]e apologize to clients who may have been affected by this. We have heightened our monitoring of accounts and increased other security measures."[5] The Chairman and CEO stated further that "[e]nsuring personal information security is fundamental to our purpose as a company of advancing financial well-being."[6]

18. SunTrust holds itself out as an institution where customers can trust that their information will be protected and secured. By way of example, SunTrust states its customer's "privacy is [SunTrust's] priority," and continues on its website:

> SunTrust understands that financial information protection is important to you, especially in today's online environment. With SunTrust's Privacy Policy, you can be assured that we use information responsibly to provide you with the services you request, and to make doing business with SunTrust easier and more convenient.
>
> There are Four things to know about financial information protection at SunTrust:
>
> 1. Because trust is critical to a solid financial relationship, SunTrust outlines exactly how and when your personal information is used in our SunTrust Privacy Policy.
> 2. You may have different ideas and expectations about privacy, which is why our consumer privacy preferences make it easy to further limit how your information is shared.
> 3. Privacy and security are a must when banking online. Our online privacy practices explain exactly how SunTrust collects, uses and protects information about your online activity.

[5] SunTrust to Offer Free Identity Protection, SunTrust Bank, Inc., http://investors.suntrust.com/news/news-details/2018/SunTrust-to-Offer-Free-Identity-Protection/default.aspx (last visited May 7, 2018)
[6] *Id.*

4. The most effective privacy protection is the precautions you take to guard your account and personal information. Review our privacy resources to learn how to protect your information.[7]

19. Moreover and in furtherance of its commitments to maintain the security and privacy of its customers' information, SunTrust states:

Who has access to your information?

•Employees of SunTrust and its subsidiaries have access to information needed to perform services on your behalf.
•SunTrust offers clients services from other firms and with your permission, shares information pertinent to those services.
•As industry practice, SunTrust provides data about your loan repayment and transactions to consumer credit bureaus.
•Federal and state laws may require us to disclose your information for specified purposes.[8]

20. Plaintiffs and the Class members would not have continued to bank with SunTrust had SunTrust told them that it lacked adequate computer systems and data security practices to safeguard customers' PII from theft. Thus, Plaintiffs and the Class members suffered actual injury and damages in paying money for access to and use of products from SunTrust that they would not have paid had SunTrust made such disclosure.

21. Plaintiffs and the Class members also suffered actual injury in the form of damages to and diminution in the value of their PII—a form of intangible property that Plaintiffs and the Class members entrusted to SunTrust for the

[7] Privacy Policy, SunTrust, https://www.suntrust.com/privacy (last visited May 7, 2018)
[8] *Id.*

purpose of accessing and using its products, which was compromised in and as a result of the Data Breach.

22. Additionally, Plaintiffs and the Class members have suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by their PII being placed in the hands of criminals who have already misused such information.

23. Moreover, Plaintiffs and the Class members have a continuing interest in ensuring that their private information, which remains in the possession of SunTrust, is protected and safeguarded from future breaches.

A. The SunTrust Data Breach Caused Harm and Will Result in Additional Fraud

24. Without detailed disclosure to SunTrust's customers, consumers, including Plaintiffs and the Class members, have been left exposed, unknowingly and unwittingly, for months to continued misuse and ongoing risk of misuse of their personal information without being able to take necessary precautions to prevent imminent harm.

25. The ramifications of SunTrust's failure to keep Plaintiffs' and Class members' data secure are severe.

26. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[9] 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."[10]

27. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[11]

28. Identity thieves can use personal information, such as that of Plaintiffs and the Class members which SunTrust failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

[9] 17 C.F.R § 248.201 (2013).
[10] *Id.*
[11] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited April 10, 2017).

29. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[12]

30. 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.[13]

31. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII or other customer data 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.[14]

32. Plaintiffs and the Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

---

[12] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited April 10, 2017).
[13] Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited April 10, 2017).
[14] GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited April 10, 2017).

Plaintiffs and the Class members are incurring and will continue to incur such damages in addition to any fraudulent activity, whether or not such injuries are ultimately reimbursed.

B. Plaintiffs and the Class Members Suffered Damages

33. Plaintiffs' and the Class members' PII is private and sensitive in nature and was left inadequately protected by SunTrust. SunTrust did not obtain Plaintiffs' and the Class members' consent to disclose their PII to any other person as required by applicable law and industry standards.

34. The SunTrust Data Breach was a direct and proximate result of SunTrust's failure to properly safeguard and protect Plaintiffs' and the Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including SunTrust's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and the Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

35. SunTrust had the resources to prevent a breach, having increased its holdings to over $205 billion as of March 31, 2018. Instead, SunTrust neglected its data security in the name of profits to its shareholders and permitted employees to

access, view, and download the PII of millions of consumers for elicit and criminal purposes.

36. Had SunTrust taken seriously its responsibilities to safeguard customers' PII, and adopted security measures recommended by experts in the field, SunTrust would have prevented the former employees' access to and, ultimately, theft of its customers' confidential PII.

37. As a direct and proximate result of SunTrust's wrongful actions and inaction and the resulting Data Breach, Plaintiffs and the Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable, for many consumers it is the way they are compensated, and even if retired from the work force, consumers should be free of having to deal with the consequences of a bank's slippage, as is the case here.

38. SunTrust's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and the Class members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their personal information being placed in the hands of criminals and sold on the Internet black market;

c. the untimely and inadequate notification of the Data Breach;

d. the improper disclosure of their PII;

e. loss of privacy;

f. money paid for access to and use of bank services during the period of the Data Breach in that Plaintiff and the Class members would not have patronized SunTrust, had SunTrust disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' financial and personal information, and had SunTrust provided timely and accurate notice of the Data Breach;

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

h. ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market;

i. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

j. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and

k. the loss of productivity and value of their time spent to address attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and

purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with all such issues resulting from the Data Breach.

39. While Plaintiffs' and the Class members' PII has been stolen, SunTrust continues to hold PII of consumers, including Plaintiffs and the Class members. Particularly because SunTrust has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiffs and the Class members have an undeniable interest in insuring their PII is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

CHOICE OF LAW

40. Georgia, which seeks to protect the rights and interests of Georgia and other U.S. residents against a company doing business in Georgia, has a greater interest in the claims of Plaintiff and the Class members than any other state, and is most intimately concerned with the claims and outcome of this litigation.

41. Atlanta is SunTrust's principal place of business, is the "nerve center" of SunTrust's business activities—the place where its high-level officers direct, control, and coordinate the corporation's activities, including its data security, and where: a) major policy; b) advertising; c) distribution; d) accounts receivable departments; and e) financial and legal decisions originate.

42. Furthermore, SunTrust's response to, and corporate decisions surrounding such response to, the Data Breach were made from and in Georgia.

43. SunTrust's breach of its duty to customers, including Plaintiffs and the Class members, emanated from Georgia.

44. Application of Georgia law to a nationwide Class with respect to Plaintiff's and the Class members' claims is neither arbitrary nor fundamentally unfair because Georgia has significant contacts and a significant aggregation of contacts that create a state interest in Plaintiffs' and the Class members' claims.

45. Further, under Georgia's choice of law principles, which are applicable to this action, the common law of Georgia will apply to the common law claims of all Class members.

CLASS ALLEGATIONS

46. Plaintiffs seek relief on behalf of themselves and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3) and (c)(4), Plaintiff seek certification of a Nationwide class defined as follows:

> All consumers residing in the United States who had financial accounts with SunTrust and any of its subsidiaries from January 1, 2018, through May 1, 2018.

47. Excluded from the Class are SunTrust and any of its affiliates, parents or subsidiaries; all SunTrust employees; all persons who make a timely election to

be excluded from the Class; government entities; and the judges to whom this case is assigned and their immediate family and court staff.

48. Plaintiffs hereby reserve the right to amend or modify the Class definition with greater specificity or division after having had an opportunity to conduct discovery.

49. The proposed Class meets the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(2), (b)(3) and (c)(4).

50. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the Class members are so numerous and geographically dispersed that the joinder of all Class members is impractical. While the exact number of Class members is unknown to Plaintiffs at this time, the proposed Class includes at least 1,500,000 customers whose data was compromised in the SunTrust Data Breach. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

51. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

a. Whether SunTrust had a duty to protect PII;

b. Whether SunTrust knew or should have known of the susceptibility of its computer systems to a data breach;

c. Whether SunTrust's security measures to protect its computer systems were reasonable in light of FTC data security recommendations, as well as other measures recommended by data security experts;

d. Whether SunTrust was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether SunTrust's failure to implement adequate data security measures allowed the breach of its computer systems to occur;

f. Whether SunTrust's conduct constituted deceptive trade practices under Georgia law;

g. Whether SunTrust's conduct, including their failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the exposure of Plaintiffs' and the Class members' PII;

h. Whether Plaintiffs and the Class members were injured and suffered damages or other acceptable losses because of SunTrust's failure to reasonably protect its computer systems and data network; and

i. Whether Plaintiffs and the Class members are entitled to relief.

52. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff's claims are typical of those of other Class members. Plaintiffs are consumers who entrusted her PII to SunTrust and had that PII compromised as a result of the Data Breach. Plaintiffs' damages and injuries are akin to other Class members and Plaintiffs seeks relief consistent with the relief of the Class.

53. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiffs are adequate representatives of the Class because Plaintiffs are members of the Class and committed to pursuing this matter against SunTrust to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, including privacy litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class' interests.

54. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Fed. R. Civ. P 23(b)(3), a class action is superior to any other available means 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. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages Plaintiffs and the Class members suffered are relatively small compared to the burden and expense required to individually litigate their claims

against SunTrust, and thus, individual litigation to redress SunTrust's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

55. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) and (c). SunTrust, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

56. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether SunTrust failed to timely notify the public of the Breach;

b. Whether SunTrust owed a legal duty to Plaintiffs and the Class members to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether SunTrust's security measures to protect its computer systems were reasonable in light of FTC data security recommendations, as well as other measures recommended by data security experts;

d. Whether Defendant failed to take commercially reasonable steps to safeguard Plaintiffs' and the Class members' PII; and,

e. Whether adherence to FTC data security recommendations, as well as measures recommended by data security experts, would have reasonably prevented the Data Breach.

57. Finally, all members of the proposed Class are readily ascertainable. SunTrust has access to information regarding which of its branches, as well as its subsidiaries' branches, were affected by the Data Breach, the time period of the Data Breach, and which customers were potentially affected. Using this information, the members of the Class can be identified and their contact information ascertained for purposes of providing notice to the Class.

COUNT I
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Nationwide Class)

58. Plaintiffs restate and reallege paragraphs 1 through [56] as if fully set forth herein.

59. SunTrust solicited and invited Plaintiffs and the Class members to access and use its financial services. Plaintiffs and the Class members accepted

SunTrust's offer and provided their PII to access and use SunTrust's financial services during the period of the Data Breach.

60. When Plaintiffs and the Class members purchased and paid for SunTrust's services, they provided their PII, including but not limited to their first and last names, addresses, social security numbers, and other highly sensitive and personal information. In so doing, Plaintiffs and the Class members entered into mutually agreed-upon implied contracts with SunTrust, pursuant to which SunTrust agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and the Class members if their data had been breached and compromised.

61. Plaintiffs and the Class members would not have provided and entrusted their PII to SunTrust to access and use their financial services in the absence of the implied contract between them and SunTrust.

62. Plaintiffs and the Class members fully performed their obligations under the implied contracts with SunTrust.

63. SunTrust's obligations under the implied contracts were to be executed in Georgia, as its corporate system and IT personnel operate out of and are located at SunTrust's "nerve center" in Georgia.

64. SunTrust breached the implied contracts it made with Plaintiffs and the Class members by failing to safeguard and protect their PII, and by failing to

provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

65. As a direct and proximate result of SunTrust's breaches of the implied contracts between SunTrust and Plaintiffs and the Class members, Plaintiffs and the Class members sustained actual losses and damages as described in detail above.

COUNT II
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

66. Plaintiffs restate and reallege paragraphs 1 through [56] as if fully set forth herein.

67. Upon accepting and storing Plaintiffs' and the Class members' PII in its computer systems and on its networks, SunTrust undertook and owed a duty to Plaintiffs and the Class Members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. SunTrust knew that the PII was private and confidential, and should be protected as private and confidential.

68. SunTrust owed a duty of care not to subject Plaintiffs and the Class members, along with their PII, to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

69. SunTrust owed numerous duties to Plaintiffs and the Class members, including the following:

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

b. to protect PII using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

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

70. SunTrust also breached its duty to Plaintiffs and the Class members to adequately protect and safeguard their PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII. Furthering their dilatory practices, SunTrust failed to provide adequate supervision and oversight of the PII with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a disgruntled employee and unknown third parties to gather Plaintiffs' and the Class members' PII, misuse that PII, and intentionally disclose it to others without consent.

71. SunTrust knew, or should have known, of the risks inherent in collecting and storing PII, and the importance of adequate security. SunTrust knew about numerous, well-publicized data breaches within the banking industry, including their own breach in 2012.

72. SunTrust knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiffs' and the Class members' PII.

73. SunTrust breached its duties to Plaintiffs and the Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and the Class members' PII.

74. Because SunTrust knew that a breach of its systems would damage millions of SunTrust customers, including Plaintiffs and the Class members, SunTrust had a duty to adequately protect its data systems and the PII contained thereon.

75. SunTrust had a special relationship with Plaintiffs and the Class members. Plaintiffs' and the Class members' willingness to entrust SunTrust with their PII was predicated on the understanding that SunTrust would take adequate security precautions. Moreover, only SunTrust had the ability to protect its systems and the PII it stored on them from unauthorized disclosure.

76. SunTrust's own conduct also created a foreseeable risk of harm to Plaintiffs, the Class members, and their PII. SunTrust's misconduct included failing to: 1) comply with industry standard security practices; 2) implement adequate system and event monitoring; and 3) implement the systems, policies, and procedures necessary to prevent this type of data breach.

77. SunTrust also had independent duties under state and federal laws that required SunTrust to reasonably safeguard Plaintiffs' and the Class members' PII and promptly notify them about the Data Breach.

78. SunTrust breached its duties to Plaintiffs and the Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and the Class members' PII;

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

c. by failing to implement adequate security systems, protocols, and practices sufficient to protect Plaintiffs' and the Class members' PII both before and after learning of the Data Breach;

d. by failing to comply with the minimum industry data security standards during the period of the Data Breach; and

e. by failing to timely and accurately disclose that Plaintiffs' and the Class members' PII had been improperly accessed and exposed.

79. Through SunTrust's acts and omissions described in this Complaint, including SunTrust's failure to provide adequate security and its failure to protect Plaintiffs' and the Class members' PII from being foreseeably captured, accessed,

disseminated, stolen, and misused, SunTrust unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiffs' and Class members' PII during the time it was within SunTrust's possession or control.

80. The law further imposes an affirmative duty on SunTrust to timely disclose the unauthorized access and theft of the PII to Plaintiffs and the Class members so they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

81. SunTrust breached its duty to notify Plaintiffs and the Class members of the unauthorized access by waiting months after learning of the Data Breach to notify Plaintiffs and the Class members, and then by failing to provide Plaintiffs and the Class members information regarding the breach until April 2018. To date, SunTrust has not provided sufficient information to Plaintiffs and the Class members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs and the Class members.

82. Through SunTrust's acts and omissions described in this Complaint, including SunTrust's failure to provide adequate security and its failure to protect Plaintiffs' and the Class members' PII from being foreseeably captured, accessed, disseminated, stolen, and misused, SunTrust unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiffs' and the Class members' PII during the time it was within SunTrust's possession or control.

83. Further, through its failure to provide timely and clear notification of the Data Breach to consumers, SunTrust prevented Plaintiffs and the Class members from taking meaningful, proactive steps to secure their financial data and bank accounts.

84. Upon information and belief, SunTrust improperly and inadequately safeguarded Plaintiffs' and the Class members' PII in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. SunTrust's failure to take proper security measures to protect sensitive PII as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiffs' and the Class members' PII.

85. SunTrust's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to Plaintiffs' and the Class members' PII; and failing to provide Plaintiffs and the Class members with timely and sufficient notice that their sensitive PII had been compromised.

86. Neither Plaintiffs nor the other Class members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint.

87. As a direct and proximate cause of SunTrust's outlined conduct, Plaintiffs and the Class members suffered damages including, but not limited to: damages arising from Plaintiffs' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach, including but not limited to late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse, and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT III
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Nationwide Class)

88. Plaintiffs restate and reallege paragraphs 1 through [56] as if fully set forth herein.

89. 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 businesses, such as SunTrust, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of SunTrust's duty in this regard.

90. SunTrust violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. SunTrust's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach at a financial institution as large as SunTrust, including, specifically, the immense damages that would result to Plaintiffs and the Class members.

91. SunTrust's violation of Section 5 of the FTC Act constitutes negligence *per se*.

92. Plaintiffs and the Class members are within the class of persons that the FTC Act was intended to protect.

93. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued 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 as that Plaintiffs and the Class members suffered.

94. As a direct and proximate result of SunTrust's negligence *per se*, Plaintiffs and the Class members have suffered, and continue to suffer, damages arising from their inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach, including but not limited to late fees charged and foregone cash back rewards; lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Nationwide Class)

95. Plaintiffs restate and reallege paragraphs 1 through [56] as if fully set forth herein.

96. Plaintiffs and the Class members conferred a monetary benefit on SunTrust. Specifically, they purchased services from SunTrust and provided SunTrust with their PII. In exchange, Plaintiffs and the Class members should have received from SunTrust access to and use of the services that were the subject of the transaction, and should have been entitled to have SunTrust protect their PII with adequate data security.

97. SunTrust knew Plaintiffs and the Class members conferred a benefit on SunTrust and accepted and has accepted or retained that benefit. SunTrust profited from the patronage and used Plaintiffs' and Class members' PII for business purposes.

98. SunTrust failed to secure Plaintiffs' and Class members' PII and, therefore, did not provide full compensation for the benefit Plaintiffs and Class members provided.

99. SunTrust acquired the PII through inequitable means when it failed to disclose the inadequate security practices previously alleged.

100. If Plaintiffs and the Class members knew SunTrust would not secure their PII using adequate security, they would not have patronized SunTrust.

101. Plaintiffs and the Class members have no adequate remedy at law.

102. Under the circumstances, it would be unjust for SunTrust to be permitted to retain any of the benefits that Plaintiffs and the Class members conferred on SunTrust.

103. SunTrust should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and the Class members, proceeds that it unjustly received from them. In the alternative, SunTrust should be compelled to refund the amounts that Plaintiffs and the Class members overpaid.

COUNT V
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Nationwide Class)

104. Plaintiffs restate and reallege Paragraphs 1 through [56] as if fully set forth herein.

105. As previously alleged, Plaintiffs and the Class members entered into an implied contract that required SunTrust to provide adequate security for the PII it collected from their enrollment in and use of SunTrust's financial services and products. As previously alleged, SunTrust owes duties of care to Plaintiffs and the Class members that require it to adequately secure PII.

106. SunTrust still possesses Plaintiffs' and the Class members' PII.

107. Although SunTrust announced that it has remedied the vulnerabilities in its computer data systems, SunTrust has not provided details of its efforts and has left Plaintiffs and the Class members to speculate as to the adequacy thereof.

108. Accordingly, SunTrust has not satisfied its contractual obligations and legal duties to Plaintiffs and the Class members. In fact, now that SunTrust's lax approach towards data security has become public, the PII in its possession is more vulnerable than previously.

109. Actual harm has arisen in the wake of the Data Breach regarding SunTrust's contractual obligations and duties of care to provide data security measures to Plaintiffs and the Class members.

110. Plaintiffs, therefore, seek a declaration that: a) SunTrust's existing data security measures do not comply with its contractual obligations and duties of care; and b) in order to comply with its contractual obligations and duties of care, SunTrust must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on SunTrust's systems on a periodic basis, and ordering SunTrust to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting customer data by, among other things, creating firewalls and access controls so that if one area of SunTrust is compromised, hackers cannot gain access to other portions of SunTrust's systems;

e. purging, deleting, and destroying in a reasonable secure manner PII not necessary for its provisions of services;

f. conducting regular database scanning and securing checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps SunTrust customers must take to protect themselves.

COUNT VI
VIOLATION OF GEORGIA FAIR BUSINESS PRACTICES ACT
O.C.G.A. § 10-1-390, *ET SEQ*.
(On Behalf of Plaintiff and the Nationwide Class)

111. Plaintiffs restate and reallege paragraphs 1 through [56] as if fully set forth herein.

112. Plaintiffs, as well as the Class members, are consumers who patronized SunTrust for its financial services and products. Therefore, Plaintiffs and

the Class members have engaged in "consumer transactions" with SunTrust, pursuant to O.C.G.A. § 10-1-392(10).

113. SunTrust is engaged in, and its acts and omissions affect, trade and commerce, pursuant to O.C.G.A. § 10-1-392(28).

114. As discussed above, SunTrust's acts, practices, and omissions at issue in this matter were directed and emanated from its headquarters in Georgia.

115. By patronizing SunTrust for access to and use of its financial services and products, Plaintiffs and the Class members entrusted SunTrust with their PII.

116. As alleged herein this Complaint, SunTrust engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including the following, in violation of the GFBPA:

a. failure to maintain adequate computer systems and data security practices to safeguard PII;

b. failure to disclose that its computer systems and data security practices were inadequate to safeguard PII from theft;

c. failure to timely and accurately disclose the Data Breach to Plaintiffs and the Class members;

d. continued acceptance of Plaintiffs' and the Class members' patronage for financial services and products, and storage of other personal information, after SunTrust knew or should have known of the security

vulnerabilities of its computer systems that were exploited in the Data Breach; and

e. continued acceptance of Plaintiffs' and the Class members' patronage for financial services and products, and storage of other personal information, after SunTrust knew or should have known of the Data Breach and before it allegedly remediated the Breach.

117. Furthermore, as alleged above, SunTrust's failure to secure consumers' PII violates the FTC Act and therefore violates the GFBPA.

118. SunTrust knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiffs' and the Class members' PII, deter hackers, deter employees from inappropriate access and dissemination, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

119. SunTrust knew or should have known that by accepting consumers' PII, Plaintiffs and the Class members would expect that SunTrust's computer and data systems were secure unless SunTrust otherwise informed them.

120. Because SunTrust offered financial services and products, and consumers entrusted SunTrust with their PII—including Plaintiffs and the Class members—Plaintiffs and the Class members expected that SunTrust's computer and data systems were secure and that their PII would be secure.

121. Accordingly, Plaintiffs and the Class members relied upon SunTrust to advise customers if its computer and data systems were not secure and, thus, PII could be compromised.

122. SunTrust did not afford Plaintiffs and the Class members equal or ample opportunity to make any inspection to determine SunTrust's data security or to otherwise ascertain the truthfulness of SunTrust's representations and omissions regarding data security, including SunTrust's failure to alert customers that its computer and data systems were not secure and, thus, were vulnerable to attack.

123. In deciding to patronize SunTrust for access to and use of its financial services and products, Plaintiffs and the Class members relied to their detriment upon SunTrust's representations and omissions regarding data security, including SunTrust's failure to alert customers that its computer and data systems were not secure and, thus, were vulnerable to attack.

124. Had SunTrust disclosed to Plaintiffs and the Class members that its computer and data systems were not secure and, thus, vulnerable to attack, Plaintiffs and the Class members would not have patronized SunTrust.

125. As a direct result of their reliance upon SunTrust to be truthful in its disclosures and non-disclosures regarding the vulnerability of its computer and data systems, Plaintiffs and the Class members patronized SunTrust and provided their

PII to SunTrust during the Data Breach period and their PII was compromised, causing Plaintiffs and the Class members to suffer damages.

126. As a direct and proximate result of SunTrust's violations of the GFBPA, Plaintiffs and the Class members suffered damages including, but not limited to: damages arising from Plaintiffs' and the Class members' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

127. Also as a direct result of SunTrust's knowing violations of the GFBPA, Plaintiffs and the Class members are entitled to damages as well as injunctive relief, including, but not limited to:

a. Ordering that SunTrust engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on SunTrust's systems on a periodic basis, and ordering SunTrust to promptly correct any problems or issues detected by such third-party security auditors;

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

c. Ordering that SunTrust audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that SunTrust segment customer data by, among other things, creating firewalls and access controls so that if one area of SunTrust is compromised, hackers cannot gain access to other portions of SunTrust's systems;

e. Ordering that SunTrust purge, delete, and destroy in a reasonable secure manner PII not necessary for its provisions of services;

f. Ordering that SunTrust conduct regular database scanning and securing checks;

g. Ordering that SunTrust routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering SunTrust to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps SunTrust customers must take to protect themselves.

128. Plaintiffs bring this action on behalf of themselves and the Class members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions, and to protect Plaintiffs, the Class members, and the public from SunTrust's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable, and unlawful practices. SunTrust's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

129. Plaintiffs and the Class members are entitled to a judgment against SunTrust for actual and consequential damages, exemplary damages and attorneys'

fees pursuant to the GFBPA, costs, and such other further relief as the Court deems just and proper.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all Class members proposed in this Complaint, respectfully request the Court enter judgment in their favor and against SunTrust as follows:

a. For an Order certifying the Class, as defined herein, and appointing Plaintiffs and their Counsel to represent the Class;

b. For equitable relief enjoining SunTrust from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and the Class members;

c. For equitable relief compelling SunTrust to use appropriate cyber security methods and policies with respect to consumer data collection, storage, and protection, and to disclose with specificity to Plaintiffs and the Class members the type of PII compromised;

d. For an award of damages, as allowed by law in an amount to be determined;

e. For an award of attorneys' fees costs and litigation expenses, as allowable by law;

f. For prejudgment interest on all amounts awarded; and

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

JURY TRIAL DEMAND

Plaintiffs demand a jury trial on all issues so triable.

This 16th day of May, 2018.

MORGAN & MORGAN, P.A.

/s/ ADIAN R. MILLER
Adian R. Miller, Esq.
Ga. Bar No.: 794647
191 Peachtree Street, N.E., Suite 4200
Post Office Box 57007
Atlanta, Georgia 30343-1007
Tel: (404) 496-7332
Fax: (404) 496-7428
armiller@forthepeople.com

MORGAN & MORGAN
COMPLEX LITIGATION GROUP
John Yanchunis *
Ryan McGee *
201 North Franklin Street, 7th Floor
Tampa, Florida 33602
Tel: (813) 223-5505
Fax: (813) 223-5402
jyanchunis@forthepeople.com
rmcgee@forthepeople.com

* *Pro Hac Vice Forthcoming*