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

JOYNEQUA WEST, individually and on behalf of herself and all others similarly situated, **Plaintiffs,** **vs.** **OVERBY-SEAWELL CO.** **and** **FULTON BANK, N.A.,** **Defendants.**	**Case No.** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Joynequa West ("Plaintiff"), on behalf of herself and all others similarly situated ("Class Members" as defined below), alleges the following Class Action Complaint against the above-captioned Defendants, Overby-Seawell Co. ("OSC") and Fulton Bank, N.A. ("Fulton Bank") (collectively, "Defendants") upon personal knowledge as to herself and her own actions, and upon information and belief, including the investigation of counsel as follows:

I. NATURE OF THE ACTION

1. This Action stems from Defendants' collective failure to secure the sensitive, personal information of their current and former customers and other consumers for whom Defendants provided services.

2. Defendant Fulton Bank, N.A., a subsidiary of Fulton Financial Corporation which is traded on the NASDAQ and is an S&P 400 Component stock, provides banking and financial services to hundreds of thousands (if not, millions) of Americans throughout Pennsylvania, Maryland, Delaware, New Jersey, and Virginia. Defendant OSC provides or provided Fulton Bank with services including ongoing verification that Fulton Bank's residential mortgage customers maintain property insurance. As a necessary part of their regular business activities Defendants collect and maintain the PII of individuals like Plaintiff and Class Members.

3. Plaintiff brings this Action on behalf of herself and all others similarly situated against Defendants for their failure to secure and safeguard sensitive personally identifiable information provided by and belonging to their customers, including: full names, mailing addresses, collateral addresses, telephone numbers, loan information (loan amount, loan maturity date, and insurance policy information) as well as Social Security numbers (collectively, the "PII").

4. According to OSC's *Notice of Data Event* (the "Notice"), sent on behalf of OSC and Fulton Bank, OSC discovered suspicious activity on their computer

systems on July 5, 2022. OSC conducted an investigation which concluded that "unauthorized access" to their servers began on May 26, 2022; and, that on July 11, 2022, their investigation concluded that PII was stolen from OSC's network.

5. In furtherance of services OSC performs on Fulton Bank's behalf, OSC obtains vast quantities of PII belonging to Fulton Bank's customers, including Plaintiff and Class Members. As such, this Action arises out of the recent targeted cyberattack against OSC that, by Defendants' own admission, allowed unauthorized third-party intruders to remotely access OSC's computer systems and data, resulting in the exfiltration of highly sensitive PII belonging to thousands of current and former Fulton Bank clients (the "Data Breach"). Additionally, the victims in this Action could number well into the millions, as numerous OSC banking clients were implicated in this Data Breach, including Defendant Fulton Bank, as well as at least one more bank (KeyBank).

6. As a result of the Data Breach, victims suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, the value of their time reasonably incurred to remedy or mitigate the effects of the attack, emotional distress, and the present and certainly imminent risk of future harm caused by the compromise of their PII.

7. As a condition of providing services, Fulton Bank requires that its customers, including Plaintiff and Class Members, entrust Fulton Bank with their

PII, including, but not limited to their names, Social Security numbers, mortgage addresses, telephone numbers, and state identification cards (e.g., Driver's Licenses, State ID Cards, or Passports), and other sensitive, non-public information.

8. As sophisticated institutions that collected, stored, and maintained the PII of Plaintiff and Class Members, Defendants owed Plaintiff and Class Members numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on their affirmative representations to keep Plaintiff's and Class Members' PII confidential, safe, secure, and protected from unauthorized disclosure, access, dissemination, or theft.

9. Indeed, during the course of its business operations, Defendants expressly and impliedly promised to safeguard Plaintiff's and Class Members' PII.

10. Furthermore, by obtaining, collecting, using, retaining, and deriving benefit from Plaintiff's and Class Members' PII, Defendants assumed legal and equitable duties to Plaintiff and Class Members and knew or should have known that they were responsible for safeguarding and protecting Plaintiff's and Class Members' PII from unauthorized disclosure access, dissemination, or theft.

11. Plaintiff and Class Members provided their PII to Fulton Bank with the reasonable expectation and mutual understanding that Fulton Bank would comply with its legal duties, obligations, and representations to keep such information confidential, safe, and secure from unauthorized access.

12. Plaintiff and Class Members reasonably expected and relied upon Fulton Bank to ensure that third party vendors to whom it entrusted their PII, like OSC, maintained adequate data security and retention systems.

13. Plaintiff and Class Members further reasonably expected and relied upon Defendants to only use their PII for business purposes, implement reasonable retention and data destruction policies, and to make only authorized disclosures of this information.

14. Plaintiff and Class Members would not have paid the amounts of money they paid for Fulton Bank's services, or surrendered their PII, had they known their information would be entrusted to and maintained by OSC, who employed inadequate data security and retention systems.

15. Defendants' data security obligations were particularly important given the substantial increase in data breaches preceding the date of the Data Breach.

16. Defendants breached their duties, promises, and obligations, and Defendants' failures to honor their obligations increased the risk that Plaintiff's and Class Members' PII would be compromised in the event of a likely cyberattack.

17. At this phase of litigation, the full extent of the types of sensitive personal information, the scope of the breach, and the root cause of the Data Breach are all within the exclusive knowledge and control of Defendants and their agents, counsel, and forensic security vendors.

18. Upon information and belief, Defendants are responsible for allowing this Data Breach through their multiple acts of negligence, including but not limited to their: failure to design, implement, and maintain reasonable data security systems and safeguards; failure to exercise reasonable care in the hiring, supervision, training, and monitoring of their employees and agents and vendors; failure to comply with industry-standard data security practices; failure to comply with federal and state laws and regulations that govern data security and privacy practices and are intended to protect the type of Sensitive Information at issue in this action; and/or failure to design, implement and execute reasonable data retention and destruction policies.

19. In this era of frequent data security attacks and data breaches, particularly in the financial industry, Defendants' failures leading to the Data Breach are particularly egregious, as this Data Breach was highly foreseeable.

20. Until notified of the breach, Plaintiff and Class Members were not aware that their PII had been compromised in the Data Breach and that they were, and continue to be, at significant risk of identity theft and various of forms of personal, social, and financial harm. This risk will remain for the remainder of their lives.

21. Plaintiff and the Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiff's and

Class Members' have heeded Defendant's warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will include into the future: reviewing financial statements, changing passwords, and signing up for credit and identity theft monitoring services, self-monitoring their accounts for instances of fraud and identity theft, and other mitigation efforts. The loss of time and other mitigation costs are tied directly to guarding against and mitigating against the imminent risk of identity theft.

22. Plaintiff and Class Members have suffered actual and present injuries as a direct result of the Data Breach, including: (a) theft of their PII; (b) costs associated with the detection and prevention of identity theft for their respective lifetimes; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of the Data Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the present and/or imminent injury arising from actual and/or potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damages to and diminution in value of their personal data entrusted to Defendants on the mutual understanding that Defendants would safeguard their PII against theft and not allow access to and misuse of their personal data by others; and (h) the continued risk to their PII, which

remains in the possession of Defendants, and which is subject to further injurious breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff and Class Members' PII. Plaintiff and Class Members, at the very least, are entitled to damages and injunctive relief tailored to address the vulnerabilities exploited in the breach, and designed to protect Plaintiff and Class Members' PII, as well as an order from the Court directing the destruction and deletion of all PII for which Defendants cannot demonstrate a reasonable and legitimate purpose for continuing to maintain possession of such PII.

23. Defendants understand the need to protect the privacy of their customers and use security measures to protect their customers' information from unauthorized disclosure. And as sophisticated financial entities who maintain private and sensitive consumer information, Defendants further understood the importance of safeguarding PII. Yet Defendants disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through access to and exfiltration by an unknown and unauthorized third party.

Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to injunctive and other equitable relief.

24. Plaintiff seeks to remedy these harms, and to prevent the future occurrence of an additional data breach, on behalf of themselves and all similarly situated persons whose PII was compromised as a result of the Data Breach. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement for loss of time, reimbursement of opportunity costs, out-of-pocket costs, price premium damages, and injunctive relief including improvements to Defendant's data security systems and protocols, future annual audits, and adequate credit monitoring services funded by the Defendant.

II. PARTIES

Plaintiff Joynequa West

25. Plaintiff West is a citizen of the state of Pennsylvania and resides in Philadelphia, Pennsylvania. Plaintiff is a consumer of Fulton Bank and provided her personal information and PII to Fulton Bank as a condition of receiving services from Fulton Bank. Fulton Bank notified Plaintiff of the Data Breach and the unauthorized access of her PII by sending her a Notice letter, dated August 30, 2022.

Defendant OSC

26. Defendant Overby-Seawell Co. is Georgia corporation and maintains its principal place of business at 245 TownPark Drive, Suite 200, Kennesaw, Georgia 30144.

Defendant Fulton Bank, N.A.

27. Defendant Fulton Bank, N.A., a subsidiary of Fulton Financial Corporation, maintains its principal place of business at One Penn Square, Lancaster, Pennsylvania 17604.

III. JURISDICTION AND VENUE

Subject Matter and Diversity Jurisdiction

28. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, and there are more than 100 members in the proposed class. The minimal diversity requirement is met as Plaintiff West and Defendant OSC are citizens of different states.

General Jurisdiction

29. OSC is a citizen of Georgia because it is a Georgia corporation and its principal place of business is in Kennesaw, Georgia. Thus, the Northern District of Georgia has general jurisdiction over OSC.

Personal Jurisdiction

30. The Northern District of Georgia has personal jurisdiction over OSC because it conducts substantial business in Georgia and this District.

31. The Northern District of Georgia has personal jurisdiction over Fulton Bank because it shared Plaintiff's and Class Members' PII with OSC and maintained significant commercial relationships in Georgia and in this District.

Venue

32. Venue is proper in this District under 28 U.S.C. §1391(b) because OSC operates in this District, Fulton Bank provided and entrusted Plaintiff's and Class Members' PII to OSC in this District, and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

IV. BACKGROUND

Defendant's Business (Fulton Bank)

33. Fulton Bank, N.A., a subsidiary of Fulton Financial Corporation which is traded on the NASDAQ and is an S&P 400 Component stock, provides banking services, including mortgage and other financial services, to hundreds of thousands (if not, millions) of Americans throughout five states on the east coast, Pennsylvania, Maryland, Delaware, New Jersey, and Virginia.

34. In the course of doing business, Defendant collects a substantial amount of PII from its consumers inclusive of the PII which was compromised in the Data Breach alleged herein.

35. Fulton Bank has acknowledged the sensitive and confidential nature of the PII it collects from its customers.

36. According to Fulton Bank's privacy policy, "your privacy is very important to us."[1] Fulton Bank also ensures its customers that "[t]o protect Personal Information from unauthorized access and use, we apply administrative, technical and physical security measures."

37. Despite promising consumers that "[w]e take our responsibility to protect your Personal Information very seriously," Fulton Bank partnered with OSC, a third-party vendor whose woefully insufficient data security policies, protocols and procedures resulted in the Data Breach and compromise of Plaintiff's and Class Members' PII.

Defendant's Business (OSC)

38. OSC, and a third-party vendor for Fulton Bank, provides or provided Fulton Bank with services including ongoing verification that Fulton Bank's residential mortgage customers maintain property insurance. OSC describes itself as a "leading provider of compliance-driven tracking technology and insurance products and services for lenders, mortgage servicers, finance companies, and property investors."

[1] https://www.fultonbank.com/Security/Consumer-Privacy-Notice, (last accessed Sept. 22, 2022).

39. In the course of doing business, OSC collects a substantial amount of PII from the consumers who do business with its banking and insurance partners, like Fulton Bank, inclusive of the PII which was compromised in the Data Breach alleged herein.

40. OSC acknowledges its duty to protect the sensitive and confidential nature of the PII it collects from the consumers who do business with its partners, like Fulton Bank and KeyBank.

41. According to OSC's published privacy policy: [2]

> The privacy of personal client information is important to [OSC]. Under Federal law, any financial institution, directly or through its affiliates, is generally prohibited from sharing nonpublic personal information about consumers or customers with a nonaffiliated third party unless the institution provides such consumer or customer with a notice of its privacy policies and practices, such as the type of information that it collects from consumers and customers and the categories of persons or entities to whom the information may be disclosed. In compliance with Federal law and the state laws relating to privacy in the insurance industry, and in order to notify our clients of our privacy policies and practices, we have established this Privacy Policy.
>
> We restrict access to nonpublic personal information about Participants to those employees of [OSC] who need to know that information in order to provide products or services to our Participants. We have in place physical, electronic, and procedural safeguards in order to protect any nonpublic personal information we maintain regarding our Participants.

[2] https://www.oscis.com/privacy/, (last accessed Sept. 22, 2022).

42. Not only does OSC claim to value privacy, but they acknowledge their obligations under "Federal law and the state laws relating to privacy in the insurance industry[.]"[3]

43. OSC's privacy policy also promises not to disclose nonpublic personal information and represents that it employs "physical, electronic, and procedural safeguards" to protect the PII it maintains –representations that are seemingly false given the Data Breach which occurred.[4]

44. Because Defendants made partial representations concerning data security, Plaintiff and Class Members relied on Defendants to fully disclose material information concerning any inadequacies in their data security practices and to disclose the foreseeable risks associated with allowing Defendants to maintain their PII.

45. Even absent these affirmative representations, Plaintiff and Class Members reasonably relied on and expected Defendants to adequately protect their PII from unauthorized access or disclosure because reasonable consumers and persons in Defendants' position understand the sensitivity of the PII and the severe consequences that result if that PII is placed in the hands of criminals, as with this Data Breach.

[3] *Id.*
[4] *Id.*

46. Plaintiff and Class Members would not have provided their PII to Defendants, or would have paid less for Defendants' services had they known that Defendants did not adequately implement or fund their data security practices.

47. Plaintiff and Class Members, relied on these express and implied promises and on these sophisticated Defendants to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, to implement reasonable retention policies, to limit access to authorized individuals, and to make only authorized disclosures of this information.

48. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendants assumed legal and equitable duties to these individuals to safeguard and protect the PII from unauthorized access.

The Data Breach

49. According to OSC's Notice letter, OSC discovered suspicious activity on their computer systems on July 5, 2022. OSC conducted an investigation which concluded that "unauthorized access" to their servers began on May 26, 2022; and, that, on July 11, 2022, their investigation concluded that PII was "stolen" from OSC's network.

50. The PII which was accessed in the Data Breach includes: full names, mailing addresses, collateral addresses, telephone numbers, loan information (loan

amount, loan maturity date, and insurance policy information) as well as Social Security numbers.

51. Upon information and belief, the PII was not encrypted or was not adequately encrypted prior to the Data Breach. Had the PII been properly encrypted, the cybercriminals would have accessed and "stolen" only useless, unintelligible data.

52. Additionally, OSC's Notice letter compounds the harm and suffering that Plaintiff and Class Members experience as a result of the Data Breach due to numerous omissions and deficiencies, including but not limited to: (1) OSC's failure to state whether the unauthorized access to their servers was terminated or whether it is on-going; (2) OSC's failure to state how hackers gained access to their servers in the first place; (3) OSC's failure to identify precisely what additional safeguards and measures they have or will implemented to ensure future protection of the PII, and notably, (3) OSC's failure to state why it waited almost 50 days from July 11, 2022 (when they first learned that PII was stolen) until August 30, 2022 to inform victims of the Data Breach.

Defendants Acquire, Collect, and Store Plaintiff's and Class Members' PII

53. Defendants acquired, collected, and stored the PII of Plaintiff and Class Members.

54. In the course and scope of its residential mortgage financing business, Fulton Bank collects, and OSC maintains, massive amounts of highly sensitive PII, likely including but not limited to, names, phone numbers, Social Security numbers, employment information (including tax returns, W-2's, pay stubs, and letters regarding employment history), assets, credit histories and letters regarding credit events, investment information, addresses, dates of birth, and driver's license information.

55. By acquiring, collecting, obtaining, and storing this information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' PII from disclosure.

56. Plaintiff and Class Members entrusted their PII to Fulton Bank on the premise and with the understanding that Fulton Bank would safeguard their information, use their PII for business purposes only, and/or not disclose their Fulton Bank to unauthorized third parties, and/or not share PII with third-party vendors, like OSC, with inadequate data security systems, and/or only retain PII for necessary business purposes and for a reasonable amount of time.

57. Plaintiff and Class Members would not have allowed Defendants, or anyone in Defendants' position, to retain their PII had they known of their inadequate data security practices.

Harm Caused by Defendants' Failure to Secure PII

58. Defendants could have prevented this Data Breach by properly securing and encrypting Plaintiff's and Class Members' PII. Additionally, Defendants could have destroyed data, including old data that Defendants had no legitimate purpose, or legal right or responsibility to retain.

59. Defendants knew that the PII they maintained was a target of data thieves and that they had a duty to protect Plaintiff's and Class Members' PII from unauthorized access.

60. In OSC's Notice letter, OSC "encourages" victims "to remain vigilant against incidents of identity theft and fraud over the next 12 to 24 months by reviewing your account statements and monitoring free credit reports for suspicious activity and to detect errors."

61. This warning is an acknowledgement by OSC that it is not only plausible that the criminals targeted and acquired the PII for criminal purposes, thereby placing the impacted customers at an imminent threat of identity theft and financial fraud – but that the theft and dissemination and misuse of the PII is the intended result of this type of cyberattack and a present threat to all Class Members.

62. This admonition also demonstrates that the "stolen" PII was unencrypted because if it had been, there would be no threat of misuse of the PII as the attackers would have exfiltrated only unintelligible data.

63. Without the likelihood of dissemination and misuse, and materialization of identity theft, the warnings and instructions to mitigate the risk would be unnecessary and would cause more harm than good, and Defendants would not have advised such actions that would cost Plaintiff and Class Members time and money unnecessarily.

64. As an additional line of protection for Plaintiff and Class Members, OSC paid for a program that offered identity theft protection services to Class Members. Absent an actual, materialized, and imminent threat to the Plaintiff and Class Members, such a program would also have been unnecessary and a waste of OSC's time and money. OSC would not have spent resources offering such a program without the likelihood that the Class Member PII was exfiltrated and disseminated in the attack, and that a materialized and imminent risk of identity theft was present for all Class Members. Even so, this identity theft protection is inadequate because it does not encompass the expected timespan during which the affected PII could be compromised (which could be for several years, if not a lifetime).

65. Defendant OSC also acknowledges their woefully insufficient data security protocols and procedures that predated the Data Breach – as they state in the Notice letter, "[w]e are taking steps to implement additional safeguards and review policies and procedures relating to data privacy and security." While OSC

essentially acknowledges that their practices needed to be improved following the Data Breach, they do not elaborate as to what those "additional safeguards … policies and procedures" are, so victims have no way of knowing whether those safeguards, policies and procedures would be sufficient to be able to protect their data (which is still in the hands of OSC) going forward.

66. What is evident and indisputable is that the Data Breach resulted in the unauthorized access of OSC's systems and theft of OSC's files, and that those compromised files contained the PII of Plaintiff and an untold number of Class Members, potentially millions.

67. Upon information and belief, the cyberattack targeted OSC due to OSC's status as a vendor for large banks, including Fulton Bank, a national, multi-billion-dollar bank, that routinely collects valuable personal and financial data on its many customers, including Plaintiff and Class Members.

68. Upon information and belief, the cyberattack was expressly designed to target and gain access to and steal the private and confidential data maintained by OSC, including the PII of Plaintiff and the Class Members.

69. As a result of the Data Breach, Plaintiff and Class Members are at an imminent risk of identity theft, fraud, and other financial crimes.

The Data Breach Was Foreseeable

70. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the financial industry and other industries holding significant amounts of PII preceding the date of the breach.

71. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendants knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

72. Indeed, cyberattacks against the financial industry have been common for over ten years with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."

73. As sophisticated financial and insurance institutions that collect, utilize, and store particularly sensitive PII, Defendants were at all times fully aware of the

increasing risks of cyber-attacks targeting the PII they controlled, and their obligation to protect the PII of Plaintiff and Class Members.

74. Plaintiff and Class Members now currently face years of having to constantly surveil and monitor their financial and personal records in addition to the loss of their privacy rights. Plaintiff and Class Members are incurring, and will continue to incur, such damages in addition to any fraudulent use of their PII.

75. The injuries to Plaintiff and Class Members are directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members, and such as encrypting the data so unauthorized third parties could not see the PII.

Defendants Failed to Protect the Plaintiff's and Class Members' PII

76. Despite the prevalence of public announcements of data breach and data security compromises, and despite Defendants' own acknowledgment of their duties to keep PII private and secure, Defendants failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

77. Fulton Bank negligently entrusted duties to safeguard Plaintiff's and Class Members' PII to OSC without performing due diligence or adequately monitoring, inspecting, or controlling OSC's data security practices.

78. Fulton Bank negligently supervised OSC and failed to successfully require OSC to implement, maintain and to sufficiently upgrade OSC's data security systems and protocols.

79. Defendants did not use reasonable security procedures and practices appropriate to the nature of the Sensitive Information it was maintaining for Plaintiff and Class Members, causing the exposure of Plaintiff's and Class Members' PII.

Defendants Failed to Comply with FTC Data Security Standards

80. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.

81. The FTC has brought well publicized enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. This includes the FTC's enforcement action against Equifax following a massive data breach involving the personal and financial information of 147 million Americans.

82. In 2016, the FTC updated its publication, "Protecting Personal Information: A Guide for Business," which established cyber-security guidelines for businesses that Defendants did not adequately employ. The FTC advised that businesses like Defendants should protect the PII that they keep by following some minimum standards related to data security, including, among others:

(a) Encrypting information stored on computer networks;

(b) Identifying network vulnerabilities;

(c) Implementing policies to update and correct any security problems;

(d) Utilizing an intrusion detection systems;

(e) Monitor all incoming traffic for suspicious activity indicating someone is attempting to hack the system;

(f) Watching for large amounts of data being transmitted from the system;

(g) Developing a response plan ready in the event of a breach;

(h) Limiting employee and vendor access to sensitive data;

(i) Requiting complex passwords to be used on networks;

(j) Utilizing industry-tested methods for security;

(k) Verifying that third-party service providers have implemented reasonable security measures;

(l) Educating and training employees on data security practices;

(m) Implementing multi-layer security including firewalls, anti- virus, and anti-malware software; and

(n) Implementing multi-factor authentication.

83. In particular, the FTC further advised that companies not maintain PII longer than is needed for authorization of a transaction: "If you don't have a legitimate business need for sensitive personally identifying information, don't keep it."

84. Upon information and belief, Defendants failed to implement or adequately implement at least one of these fundamental data security practices.

85. Defendants could have prevented this Data Breach by properly following FTC guidelines and adequately encrypting or otherwise protecting their equipment and computer files containing PII.

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

Fulton Bank Failed to Comply with the Gramm-Leach-Bliley Act

87. Fulton Bank is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

88. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [the Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

89. Fulton Bank collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Defendant was subject to the requirements of the GLBA, 15 U.S.C. § 6801.1, *et seq.*, and is subject to numerous rules and regulations promulgated on the GLBA Statutes. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. § 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

90. Accordingly, Fulton Bank's conduct is governed by the Privacy Rule prior to December 30, 2011, and by Regulation P after that date.

91. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4(a) and 313.5(a)(1); 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy

policies and practices." 16 C.F.R. § 313.4(a)(1) and 313.5(a)(1); 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9(a); 12 C.F.R. § 1016.9. As alleged herein, Fulton Bank violated the Privacy Rule and Regulation P.

92. Upon information and belief, Fulton Bank failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing and/or sharing that PII on its network.

93. Fulton Bank failed to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on its inadequately secured network and would do so after the customer relationship ended.

94. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (a) designating one or

more employees to coordinate the information security program; (b) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (c) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (d) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (e) evaluating and adjusting the information security program In light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4. As alleged herein, Fulton Bank violated the Safeguard Rule.

95. Fulton Bank failed to assess reasonably foreseeable risks to its and OSC's networks, and the security, confidentiality, and integrity of PII in its custody or control.

96. Fulton Bank failed to design and implement information safeguards to control the risks identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

97. Fulton Bank failed to adequately oversee service providers, including OSC.

98. Fulton Bank failed to evaluate and adjust its information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances.

Defendants Failed to Comply with Industry Standards

99. The financial industry also routinely incorporates these cybersecurity practices that are standard in the financial industry, and that Defendants did not adequately employ. These minimum standards include but are not limited to:

(o) Maintaining a secure firewall configuration;

(p) Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

(q) Monitoring for suspicious or irregular traffic to servers;

(r) Monitoring for suspicious credentials used to access servers;

(s) Monitoring for suspicious or irregular activity by known users;

(t) Monitoring for suspicious or unknown users;

(u) Monitoring for suspicious or irregular server requests;

(v) Monitoring for server requests for PII;

(w) Monitoring for server requests from VPNs; and

(x) Monitoring for server requests from Tor exit nodes.

100. Upon information and belief, Defendants failed to comply with at least one of these minimal industry standards, thereby opening the door to, and causing the Data Breach.

101. Defendants could have prevented this Data Breach by properly following industry data security standards by adequately encrypting or otherwise protecting their equipment and computer files containing PII.

102. Defendants could also have prevented the scale of the Data Breach simply by designing and implementing data retention practices to delete PII that is no longer needed for an ongoing business purpose.

103. Defendants had the resources necessary, and reasonable data security alternatives were known and available to Defendants that would have prevented the Data Breach, but Defendants neglected to adequately evaluate its systems, and invest in adequate security measures, despite their obligation to protect their systems and Plaintiff and Class Members' PII.

The Value of PII

104. There is both a healthy black market and a legitimate market for the type of PII that was compromised in this action. PII is such a valuable commodity to criminal networks that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

105. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the Dark Web. Numerous sources cite Dark Web pricing for stolen identity credentials. For example, personal information can be sold

at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.

106. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, when they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought.

107. The Social Security Administration has further warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, apply for a job using a false identity, open bank accounts, and apply for other government documents such as driver's license and birth certificates.

108. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for

unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are not typically discovered until an individual's authentic tax return is rejected.

109. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

110. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."

111. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x in price on the black market."

Plaintiff and Class Members Suffered Foreseeable, Concrete Harms

112. As a result of Defendants ineffective and inadequate data security and retention measures, the Data Breach, and the foreseeable consequences of the PII ending up in the possession of criminals, the risk of identity theft is materialized and imminent.

113. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/Dark Web for sale and purchase by criminals intending to utilize the PII for identity theft crimes, such as opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; or file false unemployment claims.

114. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts. The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

115. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. The fraudulent activity resulting from the Data Breach may not become evident for years.

116. Indeed, "[t]he risk level is growing for anyone whose information is stolen in a data breach." Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud." Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a later date or re-sell it.

117. To date, Defendants have done little to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in this data breach. The complimentary fraud and identity monitoring service offered by OSC is wholly inadequate as the service is only offered for 24 months and it places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

118. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must, in OSC's words, "remain vigilant" and monitor their financial accounts for many years to mitigate the risk of identity theft.

119. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts"

with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

120. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[38]

121. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.

122. Furthermore, Defendants poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Fulton Bank and/or its affiliated vendors for services, Plaintiff and Class Members understood and expected that they were paying for data security in conjunction with the services that required them to provide PII, when in fact, Defendants did not provide the

expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected.

123. As a result of Defendants' ineffective and inadequate data security and retention measures, the Data Breach, and the imminent and actual risk of identity theft, Plaintiff and Class Members have suffered numerous actual and concrete injuries, including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) deprivation of value of their PII; and (i) the continued risk to their PII, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

Plaintiff West's Experience

124. Plaintiff was required to provide and did provide her PII to Defendants during her banking relationship with Defendant Fulton Bank, and by extension, OSC.

125. To date, Defendant has done next to nothing to adequately protect

Plaintiff and Class Members, or to compensate them for their injuries sustained in this Data Breach particularly given the fact that the unencrypted PII has already been exfiltrated and likely made available to anyone wishing to download it.

126. Defendant OSC's data breach notice letter downplays the theft of Plaintiff's and Class Members PII, when the facts demonstrate that the PII was deliberately exfiltrated in a criminal action. The fraud and identity monitoring services offered by Defendant are only for two years, and Defendant places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for the service and addressing timely issues resulting from the Data Breach.

127. Plaintiff and Class Members have been further damaged by the compromise of their PII.

128. Plaintiff's PII was compromised in the Data Breach and was likely stolen and in the hands of cybercriminals who targeted and illegally accessed Defendant's network for the specific purpose of targeting the PII.

129. Plaintiff typically takes measures to protect her PII and is very careful about sharing her PII. Plaintiff has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

130. Plaintiff stores any documents containing her PII in a safe and secure location, and she diligently chooses unique usernames and passwords for her online

accounts.

131. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. In response to the Data Breach, Plaintiff has spent significant time monitoring her accounts and credit score and has sustained emotional distress in addition to her lost time. This is time that was lost and unproductive and took away from other activities and duties.

132. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to Defendants for the purpose of obtaining services from Defendants, which was compromised in and as a result of the Data Breach.

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

134. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security Number, being placed in the hands of criminals.

135. Defendants obtained and continue to maintain Plaintiff's PII and have a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Defendant Fulton Bank required the PII from Plaintiff when she

received services from Defendants. Plaintiff, however, would not have entrusted her PII to Defendants, or allowed Defendants to retain her PII, had she known that they would fail to maintain adequate data security. Plaintiff's PII was compromised, disclosed, and stolen as a result of the Data Breach.

136. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

137. Plaintiff has a continuing interest in ensuring that her PII, which upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

138. Plaintiff, pursuant to Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5), brings this Action on behalf of herself and on behalf of all other persons similarly situated. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All individuals residing in the United States whose PII was accessed or exfiltrated during the Data Breach announced by OSC in 2022 (the "Class").

139. Excluded from the Class are Defendants, any entity in which either Defendants have a controlling interest, and either Defendants' officers, directors, legal representatives, successors, subsidiaries, and agents; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and any and all federal, state or local governments, including, but not limited to, their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions. Also excluded from the Class are any judicial officers presiding over this matter, members of their immediate family, and members of their judicial staff.

140. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

141. **Numerosity, Fed R. Civ. P. 23(a)(1):** The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of thousands of individuals whose sensitive data was compromised in the Data Breach.

142. **Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3):** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

(a) Whether Defendants breached a duty to Class Members to safeguard their PII;

(b) Whether Defendants expressly or impliedly promised to safeguard the PII of Plaintiff and Class Members;

(c) Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

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

(e) Whether Defendants' data security systems prior to, during, and after the Data Breach complied with the applicable FTC data security laws and regulations;

(f) Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards, as applicable;

(g) Whether unauthorized third parties accessed or obtained Plaintiff's and Class Members' PII in the Data Breach;

(h) Whether Defendants knew or should have known that its data security systems and monitoring processes were deficient;

(i) Whether the Plaintiff and Class Members suffered legally cognizable injuries as a result of Defendants' misconduct;

(j) Whether Defendants' conduct was negligent;

(k) Whether Defendants breached expressed or implied contractual obligations;

(l) Whether Defendants violated state consumer protections statutes;

(m) Whether Defendants were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

(n) Whether Defendants failed to provide notice of the Data Breach in a timely manner;

(o) Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

(p) Whether Plaintiff and Class Members are entitled to damages, restitution, and/or civil penalties; and

(q) Whether Defendants violated state statutes as alleged herein;

143. **Typicality, Fed. R. Civ. P. 23(a)(3):** Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach due to Defendants' misfeasance, and their claims arise under the same legal doctrines.

144. **Adequacy of Representation, Fed. R. Civ. P. 23(a)(4):** Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff's counsel are competent and experienced in litigating complex class actions and data breach cases, and they intend to prosecute this action vigorously.

145. **Predominance, Fed. R. Civ. P. 23(b)(3):** Defendants have engaged in a common course of conduct toward Plaintiff and Class Members, in that all of Plaintiff and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized

issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

146. **Superiority, Fed. R. Civ. P. 23(b)(3):** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

147. **Manageability, Fed. R. Civ. P. 23(b)(3):** The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

148. **Conduct Generally Applicable to the Class, Fed. R. Civ. P. 23(b)(2):** Further, Defendants have acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate. Unless a class-wide injunction is issued, Defendants may continue in its failure to properly secure the PII of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

149. 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. The particular issues include, but are not limited to:

(a) Whether Defendants owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

(b) Whether Defendants breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

(c) Whether Defendants failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

(d) Whether an implied contract existed between Defendants on the one hand, and Plaintiff and Class Members on the other, and the terms of those implied contracts;

(e) Whether Defendants breached the implied contracts;

(f) Whether Defendants adequately, and accurately informed Plaintiff and Class Members that their PII had been compromised;

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

(h) Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members; and

(i) Whether Class Members are entitled to actual damages, statutory damages, nominal damages, injunctive relief, and/or punitive damages as a result of Defendants wrongful conduct.

VI. CAUSES OF ACTION

COUNT I

NEGLIGENCE

150. Plaintiff repeats and realleges paragraphs 1-137 as if fully set forth herein.

151. As a condition of receiving their mortgages or financial services from Defendants or their partners or affiliates, Plaintiff and the Class were obligated to provide and entrust them with certain PII, including their names, birthdates, addresses, loan numbers, Social Security numbers, and other information provided in connection with a loan application, loan modification, or other items regarding financial services.

152. Plaintiff and the Class provided and entrusted their PII to Defendants on the premise and with the mutual understanding that Defendants would safeguard

their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

153. By undertaking the duty to maintain and secure this data, sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard their systems and networks—and Plaintiff and the Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from cyber theft.

154. Defendants had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed or obtained by unauthorized parties.

155. Defendants knew or reasonably should have known that their failure to exercise due care in the collecting, storing, and using of consumers' PII involved an unreasonable risk of harm to Plaintiff and the Class, including harm that foreseeably could occur through the criminal acts of a third party.

156. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that Plaintiff's and Class Members' information in their possession was adequately secured and protected.

157. Defendants also had a duty to exercise appropriate clearinghouse practices to remove former customers' or rejected loan applicants PII that they were no longer required to retain for business purposes or pursuant to regulations.

158. Defendants had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and the Class's PII, and to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Class.

159. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between each Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendants with their confidential PII, a mandatory step in receiving services from Defendants. While this special relationship exists independent from any contract, it is recognized by Defendants' Privacy Policies, as well as applicable laws and regulations. Specifically, Defendants actively solicited and gathered PII as part of their businesses and were solely responsible for and in the position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from the resulting Data Breach.

160. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiff and the Class, to maintain adequate data security.

161. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class were all reasonably foreseeable, particularly in light of Defendants' inadequate security practices and the sensitivity of the PII they maintained.

162. Defendants also had a common law duty to prevent foreseeable harm to others. Plaintiff and the Class were the foreseeable and probable victims of Defendants' inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of adequately safeguarding that PII, and the necessity of encrypting PII stored on Defendants' systems. It was foreseeable that Plaintiff and Class members would be harmed by the failure to protect their personal information because hackers are known to routinely attempt to steal such information and use it for nefarious purposes.

163. Defendants' conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendants' wrongful conduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included their decision not to comply with industry standards for the safekeeping of Plaintiff's and the Class's PII, including basic encryption techniques available to Defendants.

164. Plaintiff and the Class had and have no ability to protect their PII that was in, and remains in, Defendants' possession.

165. Defendants were in an exclusive position to effectively protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

166. Defendants had and continue to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendants' possession was compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

167. Defendants have admitted that the PII of Plaintiff and the Class was wrongfully accessed and "stolen" by unauthorized third persons as a result of the Data Breach.

168. Defendants, through their actions and inaction, unlawfully breached their duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Class when the PII was within Defendants' possession or control.

169. Defendants improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

170. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect their current and former customers' PII in the face of increased risk of theft.

171. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of their current and former customers' PII.

172. Defendants breached their duty to exercise appropriate clearinghouse practices by failing to remove consumers' PII they were no longer required to retain pursuant to regulations.

173. Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

174. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

175. There is a close causal connection between (a) Defendants' failure to implement security measures to protect the PII of Plaintiff and the Class and (b) the harm or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and the Class's PII was accessed and exfiltrated as the direct and proximate result of

Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

176. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff's and Class Members' respective lifetimes; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and other identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the current and former customers' PII in their continued possession; and (viii) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of PII as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class Members.

177. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

178. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

179. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members are now at an increased risk of identity theft or fraud.

180. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members are entitled to and demand actual, consequential, and nominal damages and injunctive relief to be determined at trial.

COUNT II

INVASION OF PRIVACY – INTRUSION UPON SECLUSION

181. Plaintiff repeats and realleges paragraphs 1-137 as if fully set forth herein.

182. Defendants intentionally intruded into Plaintiff and Class Members' seclusion by failing to keep their PII secure.

183. By failing to keep Plaintiff and Class Members' PII secure, and allowing for access and disclosing of the PII to unauthorized parties for unauthorized use, Defendants unlawfully invaded Plaintiff and Class Members' privacy right to seclusion by, *inter alia*:

> (a) intruding into their private affairs in a manner that would be highly offensive to a reasonable persons;
>
> (b) invading their privacy by improperly using their PII properly obtained for a specific purpose for another purpose, or disclosing it to unauthorized persons;
>
> (c) failing to adequately secure their PII from disclosure to unauthorized persons; and
>
> (d) enabling the disclosure of their PII without consent.

184. The PII that was publicized during the Data Breach was highly sensitive, private, and confidential, as it included private financial and personal information.

185. There is no legitimate public interest in the disclosure of Plaintiff's and Class Members' PII.

186. As a direct and proximate result of Defendants' intrusion upon seclusion, Plaintiff and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiff and Class Members alternatively seek an award of nominal damages.

COUNT III

BREACH OF IMPLIED CONTRACT

187. Plaintiff repeats and realleges paragraphs 1-137 as if fully set forth herein.

188. Fulton Bank solicited and invited prospective customers to provide their PII to it and, by extension OSC, as part of its regular business practices. Plaintiff and the Class Members provided Fulton Bank and OSC with their PII, directly or indirectly, including their names, birthdates, addresses, loan numbers, Social Security numbers, and information provided in connection with a loan application, loan modification, or other items regarding financial services.

189. OSC acquired and maintained the PII of Plaintiff and the Class that it received from Fulton Bank. The PII included names, birthdates, addresses, loan numbers, Social Security numbers, and information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

190. When Plaintiff and Class Members provided their PII to Fulton Bank and OSC, either directly or indirectly, in exchange for goods or services, they entered into implied contracts with Fulton Bank and its vendors, including OSC, pursuant to which Fulton Bank and OSC agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

191. As a condition of receiving services, Fulton Bank, and by extension OSC, required Plaintiff and Class Members to provide their PII.

192. Pursuant to FTC guidelines and standard practice in the financial industry, Fulton Bank was obligated to take reasonable steps to maintain the security of Plaintiff's and Class Members' PII. As a result, by requesting that Plaintiff and Class Members provide their PII as part of their doing business with Fulton Bank, Fulton Bank implicitly promised to adhere to these industry standards. By entering into a third-party vendor agreement with Fulton Bank, OSC implicitly agreed to adhere to those same FTC guidelines and standard practices of the financial industry.

193. Plaintiff and Class Members each accepted Fulton Banks's offers and provided their PII to Fulton Bank, and by extension OSC. In entering into such implied contracts, Plaintiff and the Class reasonably believed that Fulton Bank's data security practices and policies, and the practices of its third-party vendors, including OSC, were reasonable and consistent with industry standards, and that Fulton Bank and OSC would use part of the fees received from Plaintiff and the Class to pay for adequate and reasonable data security practices to safeguard the PII.

194. Plaintiff and Class Members accepted Fulton Bank's offers and provided their PII to Fulton Bank, who then entrusted the PII to OSC. Defendants accepted the PII, and there was a meeting of the minds that Defendant would secure, protect, and keep the PII confidential.

195. Plaintiff fully performed their obligations under the implied contracts with Defendants.

196. Plaintiff would not have entered into transactions with Defendants if Plaintiff had known that Defendants would not protect their PII.

197. Plaintiff and the Class would not have provided and entrusted their PII to Fulton Bank, or would have paid less for its services, in the absence of the implied contract between them and Fulton Bank to keep the information secure.

198. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendants.

199. Defendants breached its implied contracts with Plaintiff and the Class by failing to safeguard and protect their PII and by failing to provide timely and accurate notice that their PII was compromised as a result of the Data Breach.

200. As a direct and proximate result of Defendants breaches of their implied contracts, Plaintiff and the Class sustained actual losses and damages as described herein and in an amount to be proven at trial.

COUNT IV

UNJUST ENRICHMENT

(Alternative to Count III)

201. Plaintiff repeats and realleges paragraphs 1-137 as if fully set forth herein.

202. When Plaintiff and Class Members paid for services and provided their PII to Fulton Bank, and by extension OSC, they did so on the mutual understanding and expectation that Defendants would use a portion of those payments, or revenue derived from the use of their PII, to adequately fund data security practices.

203. Upon information and belief, Defendants fund their data security measures entirely from their general revenues, including payments made by or on behalf of Plaintiffs and Class Members and revenue derived from the PII provided by Plaintiff and Class Members.

204. As such, a portion of the payments made by or on behalf of Plaintiffs and Class Members, or the revenue derived from their PII, is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

205. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII and instead directing those funds to their own profits. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendants instead calculated to increase their own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate

result of Defendants' decision to prioritize their own profits over the requisite security.

206. Defendants knew that Plaintiff and Class Members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

207. For years and continuing to today, Defendants' business models have depended upon their use of consumers' PII. Trust and confidence are critical and central to the services provided by Defendants in the residential financing industry. Unbeknownst to Plaintiff and absent Class Members, however, Defendants did not secure, safeguard, or protect its customers' and employees' data and employed deficient security procedures and protocols to prevent unauthorized access to customers' PII. Defendants' deficiencies described herein were contrary to their security messaging.

208. Plaintiff and Class Members received services from Defendants, and Defendants were provided with, and allowed to collect and store, their PII on the mistaken belief that Defendants complied with their duties to safeguard and protect its customers' and employees' PII. Upon information and belief, putting their short-term profit ahead of safeguarding PII, and unbeknownst to Plaintiff and absent Class Members, Defendants knowingly sacrificed data security to save money.

209. Upon information and belief, Defendants knew that the manner in which they maintained and transmitted customer PII violated industry standards and their fundamental duties to Plaintiff and absent Class Members by neglecting well-accepted security measures to ensure confidential information was not accessible to unauthorized access. Defendants had knowledge of methods for designing safeguards against unauthorized access and eliminating the threat of exploit, but it did not use such methods.

210. Defendants had within their exclusive knowledge, and never disclosed, that they had failed to safeguard and protect Plaintiff and absent Class Members' PII. This information was not available to Plaintiff, absent Class Members, or the public at large.

211. Defendants also knew that Plaintiff and Class Members expected security against known risks and that they were required to adhere to state and federal standards for the protection of confidential personally identifying, financial, and other personal information.

212. Plaintiff and absent Class Members did not expect that Defendants would knowingly insecurely maintain and hold their PII when that data was no longer needed to facilitate a business transaction or other legitimate business reason. Likewise, Plaintiff and absent Class Members did not know or expect that

Defendants would employ substantially deficient data security systems and fail to undertake any required monitoring or supervision of the entrusted PII.

213. Had Plaintiff and absent Class Members known about Defendants' efforts to deficiencies and efforts to hide their ineffective and substandard data security systems, Plaintiff and absent Class Members would not have entered into business dealings with Defendants.

214. By withholding the facts concerning the defective security and protection of customer PII, Defendants put their own interests ahead of the very customers who placed their trust and confidence in Defendants, and benefitted themselves to the detriment of Plaintiff and absent Class Members.

215. As a result of its conduct as alleged herein, Defendants sold more services than it otherwise would have, and was able to charge Plaintiff and Class Members more for mortgage services than it otherwise could have. Defendants were unjustly enriched by charging for and collecting for those services that it would not have obtained to the detriment of Plaintiff and absent Class Members.

216. It would be inequitable, unfair, and unjust for Defendants to retain these wrongfully obtained fees and benefits. Defendants' retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

217. Defendants' unfair and deceptive conduct to not disclose those defects have, among other things, caused Plaintiff and Class Members to enter a business arrangement that was deceptive and dangerous to their identities.

218. As a result, Plaintiff paid for services that they would not have paid for had Defendants disclosed the inadequacy of its data security practices.

219. Plaintiff and each Member of the proposed Class are each entitled to restitution and non-restitutionary disgorgement in the amount by which Defendants were unjustly enriched, to be determined at trial.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying the Class and appointing Plaintiff and her counsel to represent the certified Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

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

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

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

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII;

v. prohibiting Defendants from maintaining Plaintiff's and Class Members' PII on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering

Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

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

xii. requiring Defendants to conduct internal training and education routinely and continually, and on an annual basis to inform internal

security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

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

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants servers; and

xvii. for a period of ten years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis

to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment.

D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined

E. For an award of damages, including a sum of money sufficient to provide to Plaintiff and Class Members identity theft protection services for their respective lifetimes.

F. For an award of punitive damages;

G. For an award of attorneys' fees, costs, and litigation expenses pursuant to O.C.G.A. Section 13-6-11 and as otherwise allowed by law;

H. For prejudgment interest on all amounts awarded; and

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

VIII. JURY TRIAL DEMAND

A jury trial is demanded by Plaintiff and the Class Members as to all issues so triable.

Respectfully submitted this 26th day of September, 2022.

/s/ MaryBeth V. Gibson

MaryBeth V. Gibson
Georgia Bar No. 725843
THE FINLEY FIRM, P.C.
3535 Piedmont Rd.
Building 14, Suite 230
Atlanta, GA 30305
Phone: (404) 978-6971
Fax: (404) 320-9978
mgibson@thefinleyfirm.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: 866.252.0878
gklinger@milberg.com

Attorneys for Plaintiff and the Classes

**Pro Hac Vice forthcoming*

CERTIFICATE OF COMPLIANCE

I certify that the foregoing pleading has been prepared with Times New Roman, 14-point font, in compliance with L.R. 5.1B.

/s/ MaryBeth V. Gibson

MARYBETH V. GIBSON