**UNITED STATES DISTRICT COURT**
**DISTRICT OF MASSACHUSETTS**

| | |
|---|---|
| **STEVE SELLIN**, individually and on behalf of all other similarly situated individuals,<br><br>Plaintiff,<br><br>v.<br><br>**STAPLES, INC.**,<br><br>Defendant. | Case No. _____<br><br>**JURY TRIAL DEMANDED** |

Plaintiff Steve Sellin ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint and alleges the following against Defendant Staples, Inc. ("Defendant"), based upon personal knowledge with respect to Plaintiff and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

## SUMMARY OF THE CASE

1. Plaintiff brings this class action against Defendant for its failure to properly secure Plaintiff's and Class Members' personally identifiable information ("PII" or "Private Information").

2. Defendant is an office supply retail company.

3. Plaintiff and Class Members were required to provide Defendant with their Private Information in connection with obtaining services and/or employment from Defendant.

4. On March 11, 2026, the ransomware group CoinbaseCartel publicly claimed responsibility for a cyberattack against Defendant ("Data Breach").[1] The group posted an extortion notice indicating that sensitive data would be leaked unless negotiations were initiated.[2]

[1] https://www.dexpose.io/coinbasecartel-strikes-staples-inc/.
[2] *Id.*

5. CoinbaseCartel claims to have over 2TB of data from the Data Breach.[3]

6. Upon information and belief, the Private Information of Plaintiff and Class Members exposed in the Data Breach includes names, addresses, dates of birth, and/or Social Security numbers.

7. Upon information and belief, Plaintiff's Private Information is available on the Dark Web as a result of the Data Breach.

8. Upon information and belief, due to Defendant's negligence, cybercriminals have accessed and obtained everything they need to commit identity theft and wreak havoc on the personal lives of thousands of individuals including Plaintiff.

9. Defendant knowingly obtained Plaintiff's and Class Members' sensitive Private Information and had a resulting duty to securely maintain that information in confidence. Plaintiff and Class Members would not have provided their Private Information to Defendant if they had known that Defendant would not ensure that it used adequate security measures.

10. By taking possession and control of Plaintiff's and Class members' Private Information, Defendant assumed a duty to securely store and protect it.

11. Now, and for the rest of their lives, Plaintiff and the Class Members will have to deal with the danger of identity thieves possessing and misusing their Private Information. Even those Class Members who have yet to experience identity theft have to spend time responding to the Data Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiff and Class Members have incurred and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit,

[3] https://x.com/DarkWebInformer/status/2031835544942940332/photo/1.

deprivation of the value of their Private Information, loss of privacy, and/or additional damages as described below.

12. In sum, Plaintiff and the Class will face an imminent risk of fraud and identity theft for the rest of their lives because: (i) Defendant failed to protect Plaintiff's and the Class's Private Information, allowing a large and preventable Data Breach to occur; (ii) the cybercriminals who perpetrated the Breach accessed Private Information that they will sell on the dark web (if they have not already) because that is the *modus operandi* of cybercriminals who perpetrate breaches such as this; and (iii) Plaintiff and Class members are at immediate risk of experiencing misuse of their Private Information.

13. Plaintiff seeks to remedy these harms individually and on behalf of all other similarly situated individuals whose Private Information was exposed in the Data Breach. Plaintiff seeks remedies including compensation for time spent responding to the Data Breach and other types of harm, free credit monitoring and identity theft insurance, and injunctive relief including substantial improvements to Defendant's data security policies and practices.

## JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because (a) the aggregate amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs (b) the action is a class action (c) there are Class members who are diverse from Defendant, including Plaintiff, who is a citizen of Kentucky, and (d) there are more than 100 Class members.

15. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1) and because Defendant resides in this District.

## PARTIES

17. Plaintiff is a citizen and resident of Lexington, Kentucky, where he intends to remain.

18. Defendant is a Delaware corporation with its principal place of business located at 500 Staples Drive, Framingham, MA 01702.

## FACTUAL ALLEGATIONS

### A. Background on Defendant

19. Defendant is an American office supply retail company.

20. Due to the nature of the services it provides, Defendant acquires and electronically stores Private Information. Defendant was therefore required to ensure that Private Information was not disclosed or disseminated to unauthorized third parties without Plaintiff's and Class Members' express written consent. Defendant has a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties, including in selecting its vendors, encrypting the information, and purging information once it is no longer needed.

21. Upon information and belief, Defendant made promises and representations to Plaintiff and Class Members, including through its Privacy Policies, that Private Information collected from them, including that of Plaintiff and Class Members, would be kept save and confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

### B. The Data Breach

22. On March 11, 2026, the ransomware group CoinbaseCartel publicly claimed responsibility for a cyberattack against Defendant by posting an extortion notice.

23. Several facts may be gleaned from extortion notice, including: a) the Data Breach was the work of cybercriminals; b) the cybercriminals first infiltrated Defendant's networks and systems, and downloaded data from the networks and systems (aka exfiltrated data, or in layperson's terms "stole" data; and c) that once inside Defendant's networks and systems, the cybercriminals targeted information including Plaintiff's and Class Members' Private Information and other sensitive information for download and theft.

24. There is no indication that Defendant has undertaken any efforts to contact the Class Members whose data was accessed and acquired in the Data Breach to inquire whether any of the Class Members suffered misuse of their data, whether Class Members should report their misuse to Defendant, and whether Defendant set up any mechanism for Class Members to report any misuse of their data.

25. Defendant failed to take precautions designed to keep individuals' Private Information secure.

26. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

27. Plaintiff further believes the Private Information of Class Members was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this nature.

**C. Data Breaches Are Preventable.**

28. Data breaches are preventable.[4] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security

[4] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," in DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

solutions."[5] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[6]

29. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures . . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs." [7]

30. Defendant could have prevented this Data Breach by, among other things, properly encrypting, redacting, or otherwise protecting their equipment and computer files containing Private Information.

31. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[8]

32. To prevent and detect cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

[5] *Id.* at 17.
[6] *Id.* at 28.
[7] *Id.*
[8] How to Protect Your Networks from RANSOMWARE, at 3, *available at:* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[9]

33. To prevent and detect cyber-attacks or ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

**Secure internet-facing assets**

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

**Thoroughly investigate and remediate alerts**

- Prioritize and treat commodity malware infections as potential full compromise;

**Include IT Pros in security discussions**

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

**Build credential hygiene**

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

**Apply principle of least-privilege**

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

[9] *Id.* at 3-4.

**Harden infrastructure**

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[10]

34. Given that Defendant was storing the sensitive Private Information of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

35. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of, upon information and belief, hundreds and possibly even thousands of individuals, including that of Plaintiff and Class Members.

**D. Defendant Acquires, Collects, and Stores Individuals' Private Information**

36. In connection with the services and employment Defendant provides, Plaintiff and Class Members were required to give their sensitive and confidential Private Information to Defendant.

37. Defendant retains and stores this information and derives a substantial economic benefit from the Private Information that it collects. But for the collection of Plaintiff's and Class Members' Private Information, Defendant would be unable to carry out its regular business operations.

[10] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

38. By obtaining, collecting, and storing the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

39. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

40. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiff and Class Members.

**E. The Data Breach Was Foreseeable and the Defendant Was Aware of Its Risk**

41. It is well known that Private Information is an invaluable commodity and a frequent target of hackers.

42. In 2024, 3,158 data breaches occurred, exposing approximately 1,350,835,988 sensitive records—a 211% increase year-over-year.[11]

43. Individuals place a high value not only on their Private Information, but also on the privacy of that data. For the individual, identity theft causes significant negative financial impact on victims as well as severe distress and other strong emotions and physical reactions.

44. In light of recent high profile data breaches at other industry-leading companies, Defendant knew or should have known that the Private Information that it collected and maintained would be targeted by cybercriminals.

[11] *2024 Data Breach Report*, ITRC (Identity Theft Resource Center) (January 2025), *available at* https://www.idtheftcenter.org/publication/2024-data-breach-report/.

45. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

46. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

47. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

48. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

49. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

50. As an entity in possession of Plaintiff's and Class Members' Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class Members and of the foreseeable consequences if its data security systems and network were breached. This includes the significant costs imposed on Plaintiff and Class Members because of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

**F. The Value of Private Information**

51. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[12] 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," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[13]

52. The PII of individuals 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.[14]

53. For example, Personal Information can be sold at a price ranging from $40 to $200.[15] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[16]

54. Of course, a stolen Social Security number – standing alone – can be used to wreak untold havoc upon a victim's personal and financial life. The popular person privacy and credit monitoring service LifeLock by Norton notes "Five Malicious Ways a Thief Can Use Your Social Security Number," including 1) Financial Identity Theft that includes "false applications for loans, credit cards or bank accounts in your name or withdraw money from your accounts, and

---

[12] 17 C.F.R. § 248.201 (2013).
[13] *Id.*
[14] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.
[15] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.
[16] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

which can encompass credit card fraud, bank fraud, computer fraud, wire fraud, mail fraud and employment fraud; 2) Government Identity Theft, including tax refund fraud; 3) Criminal Identity Theft, which involves using someone's stolen Social Security number as a "get out of jail free card;" 4) Medical Identity Theft, and 5) Utility Fraud.

55. It is little wonder that courts have dubbed a stolen Social Security number as the "gold standard" for identity theft and fraud. Social Security numbers, which were compromised in the Data Breach, are among the worst kind of Private Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

56. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases." [17] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[18]

57. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and Class Members, 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, 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. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[19]

---

[17] *See* https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases.

[18] *Id.*

[19] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf.

58. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[20] "Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits."[21]

59. 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.

60. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[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."[22]

61. For these reasons, some courts have referred to Social Security numbers as the "gold standard" for identity theft. *Portier v. NEO Tech. Sols*., No. 3:17-CV-30111, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) ("Because Social Security numbers are the gold standard for identity theft, their theft is significant . . . . Access to Social Security numbers causes long-lasting jeopardy because the Social Security Administration does not normally replace Social Security numbers."), report and recommendation adopted, No. 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *see also McFarlane v. Altice USA, Inc*., 2021 WL 860584, at

[20] *See* https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/.
[21] *See* https://www.investopedia.com/terms/s/ssn.asp.
[22] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft.

*4 (citations omitted) (S.D.N.Y. Mar. 8, 2021) (the court noted that Plaintiff' Social Security numbers are: arguably "the most dangerous type of personal information in the hands of identity thieves" because it is immutable and can be used to "impersonat[e] [the victim] to get medical services, government benefits, ... tax refunds, [and] employment." . . . Unlike a credit card number, which can be changed to eliminate the risk of harm following a data breach, "[a] social security number derives its value in that it is immutable," and when it is stolen it can "forever be wielded to identify [the victim] and target his in fraudulent schemes and identity theft attacks.")

62. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[23]

63. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security numbers, dates of birth, and names.

64. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

65. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also

[23] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[24]

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

**G. Defendant Failed to Comply with FTC Guidelines**

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

68. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should: (i) protect the personal customer information that they keep; (ii) properly dispose of personal information that is no longer needed; (iii) encrypt information stored on computer networks; (iv) understand their network's vulnerabilities; and (v) implement policies to correct security problems.

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

70. The FTC recommends that companies not maintain information longer than is

[24] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf.

needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

71. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

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

**H. Defendant Failed to Follow Industry Standards**

73. Experts studying cybersecurity routinely identify companies such as Defendant's as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

74. Several best practices have been identified that—at a minimum—should be implemented by businesses like Defendant. These industry standards include: educating all employees regarding cybersecurity; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

75. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email

management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; protecting against any possible communication system; and training staff regarding critical points.

76. Moreover, companies should retain personal data only as necessary, with legal justification. Personal data should not be stored beyond the time necessary to achieve its initial purpose of collection. In line with industry standard practices, Defendant should have promptly deleted any data it no longer needed as it relates to Plaintiff and the Class.

77. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO04), which are established standards in reasonable cybersecurity readiness.

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

## I. The Data Breach Caused Injury to Class Members and Will Result in Additional Harm Such as Fraud.

79. Without detailed disclosure to the victims of the Data Breach, individuals whose Private Information was compromised by the Data Breach, including Plaintiff and Class Members, were unknowingly and unwittingly exposed to continued misuse and ongoing risk of misuse of their Private Information for months without being able to take available precautions to prevent imminent harm.

80. The ramifications of Defendant's failure to secure Plaintiff's and Class Members' data are severe.

81. Victims of data breaches are much more likely to become victims of identity theft and other types of fraudulent schemes. This conclusion is based on an analysis of years of data that correlated each year's data breach victims with those who also reported being victims of identity fraud.

82. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[25] 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."[26]

83. Identity thieves can use Private Information, such as that of Plaintiff and Class Members, which Defendant 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.

84. As demonstrated herein, these and other instances of fraudulent misuse of the compromised Private Information have already occurred and are likely to continue.

85. 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

[25] 17 C.F.R. § 248.201 (2013).
[26] *Id*.

2014.[27]

86. The 2017 Identity Theft Resource Center survey[28] evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed;
- 67% reported anxiety;
- 66% reported feelings of fear related to personal financial safety;
- 37% reported fearing for the financial safety of family members;
- 24% reported fear for their physical safety;
- 15.2% reported a relationship ended or was severely and negatively impacted by identity theft; and
- 7% reported feeling suicidal.

87. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate / lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[29]

[27] *Victims of Identity Theft*, Bureau of Justice Statistics (Sept. 2015) http://www.bjs.gov/content/pub/pdf/vit14.pdf
[28] *Id.*
[29] *Id.*

88. Given the type of targeted attack in this case, the sophisticated criminal activity, the volume of data compromised in this Data Breach, and the sensitive type of Private Information involved in this Data Breach, 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 Private Information for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

89. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

90. Consequently, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

91. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft resulting from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear, but for Defendant's failure to safeguard their Private Information.

**J. Plaintiff and Class Members Suffered Damages.**

92. As a direct and proximate result of Defendant's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class Members have already been harmed by the fraudulent misuse of their Private Information, and have been placed at an imminent, immediate, and continuing increased risk of additional 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 family in an effort to mitigate both the actual and potential impact of the Data Breach on their lives. Such mitigatory actions include, *inter alia*, 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, sorting through dozens of phishing and spam email, text, and phone communications, and filing police reports. This time has been lost forever and cannot be recaptured.

93. Defendant's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' Private Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft and misuse of their personal and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals and misused via the sale of Plaintiff's and Class Members' information on the Internet's black market;

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

d. the improper disclosure of their Private Information;

e. loss of privacy;

f. 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;

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

h. 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 inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data Breach; and

i. nominal damages.

94. While Plaintiff's and Class Members' Private Information has been stolen, Defendant continues to hold Plaintiff's and Class Members' Private Information. Particularly because Defendant has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and Class Members have an undeniable interest in ensuring that their Private Information is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

**K. Plaintiff's Experience and Injuries.**

95. At all times relevant, Plaintiff is a former employee of Defendant.

96. As a condition of receiving employment from Defendant, Plaintiff was required to provide his sensitive Private Information to Defendant.

97. Plaintiff provided his Private Information to Defendant and trusted that it would use reasonable measures to protect it according to state and federal law.

98. Plaintiff's Private Information was in Defendant's possession at the time of the Data Breach.

99. As a result of its inadequate cybersecurity measures and data destruction policies, Defendant exposed Plaintiff's Private Information for theft by cybercriminals and given the

purpose of the hack, for sale on the Dark Web.

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

101. Plaintiff suffered actual injury from the exposure of his Private Information — which violates his rights to privacy.

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

103. As a result of the Data Breach, Plaintiff has spent time and made reasonable efforts to mitigate its impact, including but not limited to researching the Data Breach, reviewing credit card and financial account statements and monitoring his credit information.

104. Plaintiff will continue to spend considerable time and effort monitoring his accounts to protect himself from identity theft. Plaintiff fears for his personal financial security and uncertainty over what Private Information was exposed. Plaintiff has and is experiencing feelings of stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

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

106. Once an individual's Private Information is for sale and access on the Dark Web, cybercriminals are able to use the stolen and compromised information to gather and steal even more information. Plaintiff's Private Information was compromised as a result of the Data Breach.

107. Plaintiff has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

108. Plaintiff also has a continuing interest in lifetime credit monitoring and identity theft monitoring on account of the Data Breach.

## CLASS ALLEGATIONS

109. Plaintiff brings this class action individually on behalf of himself and all members of the following Class of similarly situated persons pursuant to Federal Rule of Civil Procedure 23. Plaintiff seeks certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3) of the following class:

> All persons residing in the United States whose Private Information was compromised in the Data Breach and received Notice ("Class"):

110. Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, officers, agents, and directors, any entities in which Defendant has a controlling interest, as well as the judge(s) presiding over this matter and the clerks, judicial staff, and immediate family members of said judge(s).

111. Plaintiff reserves the right to modify or amend the foregoing Class definitions before the Court determines whether certification is appropriate.

112. Numerosity: The members in the Class are so numerous that joinder of all Class Members in a single proceeding would be impracticable. Upon information and belief, Plaintiff believes the number of affected individuals is in the thousands.

113. Commonality and Predominance: Common questions of law and fact exist as to all Class Members and predominate over any potential questions affecting only individual Class Members. These common questions of law or fact include, *inter alia*:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class Members' Private Information from unauthorized access and disclosure;

c. Whether Defendant's computer systems and data security practices used to protect Plaintiff's and Class Members' Private Information violated the FTC Act and/or state laws, and/or Defendant's other duties discussed herein;

d. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and Class Members;

e. Whether Defendant unlawfully shared, lost, or disclosed Plaintiff's and Class Members' Private Information;

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

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

h. Whether Plaintiff and Class Members suffered injury as a proximate result of Defendant's negligent actions or failures to act;

i. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' Private Information;

j. Whether Defendant breached duties to protect Plaintiff's and Class Members' Private Information;

k. Whether Defendant's actions and inactions alleged herein were negligent;

l. Whether Defendant was unjustly enriched by its conduct as alleged herein;

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

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

114. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff on behalf of himself and all other Class Members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

115. Typicality: Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had his Private Information compromised in the Data Breach. Plaintiff and Class Members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class Members.

116. Adequacy: Plaintiff will fairly and adequately protect the interests of the Class Members. Plaintiff is an adequate representative of the Class and has no interests adverse to, or in conflict with, the Class he seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

117. Superiority: 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 damages and other financial detriment suffered by Plaintiff and all other Class Members are relatively small compared to the burden and expense

that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class Members to individually seek redress from Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation creates a 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 single adjudication, economy of scale, and comprehensive supervision by a single court.

118. Injunctive and Declaratory Relief: Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

119. Likewise, particular issues are appropriate for certification under Rule 24(c)(4) 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 issues include, but are not limited to: (a) whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, and safeguarding their Private Information; (b) whether Defendant failed to adequately monitor and audit their data security systems; and (c) whether Defendant failed to take reasonable steps to safeguard the Private Information of Plaintiff and Class Members.

120. All members of the proposed Class are readily ascertainable. Defendant has access to the names in combination with addresses and/or e-mail addresses of Class Members affected by the Data Breach.

## CAUSES OF ACTION

### COUNT I
### NEGLIGENCE
### (On Behalf of Plaintiff and the Class)

121. Plaintiff restates and realleges paragraphs 1 through 120, above as if fully set forth herein.

122. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and 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. That duty included, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff's and Class Members' Private Information in Defendant's possession was adequately secured and protected, that Plaintiff's and Class Members' Private Information on Defendant's networks was not accessible to criminals without authorization, and that Defendant's employees tasked with maintaining such information were adequately trained on security measures regarding the security of Plaintiff's and Class Members' Private Information.

123. Plaintiff and Class Members entrusted their Private Information to Defendant with the understanding that Defendant would safeguard their information, use their Private Information for business purposes only, and not disclose their Private Information to unauthorized third parties.

124. Defendant knew or reasonably should have known that a failure to exercise due care in the collecting, storing, and using Plaintiff's and Class Members' Private Information involved an unreasonable risk of harm to Plaintiff and Class Members.

125. Defendant had a duty to protect Plaintiff's and the Class Members' Private Information as the custodian of their Private Information, which Plaintiff and Class Members

were required to submit to Defendant in connection with the services Defendant provides.

126. Defendant had a duty to comply with industry standard data protection and policy measures and the FTC Act in its collection, storage, and management of Private Information.

127. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' Private Information.

128. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly in light of prior data breaches and disclosures prevalent in today's digital landscape.

129. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing Plaintiff's and Class Members' Private Information, the critical importance of providing adequate security of that information, the necessity for encrypting Private Information stored on Defendant's systems, and that it had inadequate IT security protocols in place to secure Plaintiff's and Class Members' Private Information.

130. Defendant's misconduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, failure to take the steps and opportunities to prevent the Data Breach as set forth herein.

131. Plaintiff and Class Members had no ability to protect their Private Information that was in Defendant's possession.

132. Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

133. Defendant had a duty to timely disclose that Plaintiff's and Class Members' Private Information within its possession was compromised and precisely the type(s) of information that were compromised. Defendant breached this duty by failing to disclose the Data

Breach within a reasonable time.

134. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' Private Information.

135. Defendant systematically failed to provide adequate security for data in its possession.

136. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within its possession.

137. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' Private Information.

138. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the Private Information within its possession might have been compromised and precisely the type of information compromised.

139. Defendant's breach of its duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised.

140. But for all of Defendant's acts of negligence detailed above, including allowing cyber criminals to access its systems containing Plaintiff's and Class Members' Private Information would not have been compromised.

141. Plaintiff never transmitted his own unencrypted Private Information over the internet or any other unsecured source.

142. Following the Data Breach, Plaintiff's Private Information has been seized by unauthorized third parties who are now free to exploit and misuse that Private Information, and Plaintiff is unable to prevent its further dissemination. Plaintiff's Private Information is forever

compromised.

143. But for the Data Breach, Plaintiff would not have incurred the loss and publication of his Private Information and other injuries.

144. There is a close causal connection between Defendant's failure to implement security measures to protect Plaintiff's and Class Members' Private Information and the harm suffered, or risk of imminent harm suffered by Plaintiff and Class Members. Plaintiff's and Class Members' Private Information was accessed and compromised as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures and encryption.

145. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, loss of privacy, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

146. As a result of Defendant's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

147. Plaintiff seeks the award of actual damages on behalf of himself and the Class.

148. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order (1) compelling Defendant to institute appropriate data collection and safeguarding methods and policies with regard to Private Information; and (2) compelling Defendant to provide detailed and specific disclosure of what types of Private Information have been compromised as a result of the data breach.

**COUNT II**
**NEGLIGENCE *PER SE***
**(On Behalf of Plaintiff and the Class)**

149. Plaintiff restates and realleges paragraphs 1 through 120, above as if fully set forth herein.

150. Pursuant to the FTC Act, Defendant was required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and Class Members' Private Information.

151. Defendant breached its duties by failing to employ industry standard data and cybersecurity measures to ensure their compliance with federal and state laws, the FTC Act, and its internal Privacy Policies by, including, but not limited to, failing to employ proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

152. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Defendant's networks, databases, and computers that stored or contained Plaintiff's and Class Members' Private Information.

153. Defendant's violations of the FTC Act constitute negligence *per se*.

154. Plaintiff and Class Members are within the category of persons the FTC Act is intended to protect.

155. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act is intended to guard against.

156. Plaintiff's and Class Members' Private Information constitutes personal property that was stolen due to Defendant's negligence, resulting in harm, injury, and damages to Plaintiff and Class Members.

157. Defendant's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiff's and Class Members' unencrypted Private Information, and Plaintiff and Class Members have suffered and will continue to suffer damages as a result of Defendant's conduct. Plaintiff and Class Members seek damages and other relief as a result of Defendant's negligence.

## COUNT III
## BREACH OF IMPLIED CONTRACT
## (On Behalf of Plaintiff and the Class)

158. Plaintiff restates and realleges paragraphs 1 through 120 above as if fully set forth herein.

159. When Plaintiff and Class Members provided their Private Information to Defendant, they entered into implied contracts with Defendant, under which Defendant agreed to take reasonable steps to protect Plaintiff's and Class Members' Private Information, comply with its statutory and common law duties to protect Plaintiff's and Class Members' Private Information, and to timely notify them in the event of a data breach.

160. Defendant solicited and invited Plaintiff and Class Members to provide their Private Information as part of Defendant's provision of services and/or employment. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

161. When entering into implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with its statutory and common law duties to adequately protect Plaintiff's and Class Members' Private Information and to timely notify them in the event of a data breach.

162. Defendant's implied promise to safeguard Private Information is evidenced by, *e.g.*, the representations in its Privacy Policies.

163. Plaintiff and Class Members would not have provided their Private Information to Defendant had they known that Defendant would not safeguard their Private Information, as promised, or provide timely notice of a data breach.

164. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendant.

165. Defendant breached its implied contracts with Plaintiff and Class Members by failing to safeguard Plaintiff's and Class Members' Private Information and by failing to provide them with timely and accurate notice of the Data Breach.

166. The losses and damages Plaintiff and Class Members sustained, include, but are not limited to:

a. Theft of their Private Information;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their Private Information;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling, and reissuing cards, enrolling in credit monitoring and identity theft

protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of Private Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

167. As a direct and proximate result of Defendant's breach of contract, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

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

168. Plaintiff restates and realleges paragraphs 1 through 120, above as if fully set forth herein.

169. Plaintiff and Class Members have an interest, both equitable and legal, in their Private Information that was conferred upon, collected by, and maintained by Defendant and that was stolen in the Data Breach.

170. Defendant benefitted from the conferral upon it of Plaintiff's and Class Members' Private Information, and by its ability to retain and use that information. Defendant understood that it so benefited.

171. Defendant also understood and appreciated that Plaintiff's and Class Members' Private Information was private and confidential and that its value depended upon Defendant maintaining its privacy and confidentiality.

172. But for Defendant's willingness and commitment to maintain its privacy and confidentiality, that Private Information would not have been transferred to and entrusted with Defendant. Further, if Defendant had disclosed that its data security measures were inadequate, Defendant would not have been permitted to continue in operation by regulators and the financial marketplace.

173. As a result of Defendant's wrongful conduct as alleged in this Complaint (including, among other things, its failure to employ adequate data security measures, its continued maintenance and use of Plaintiff's and Class Members' Private Information without having adequate data security measures, and its other conduct facilitating the theft of that Private Information), Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members.

174. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compilation and use of Plaintiff's and Class Members' sensitive Private Information, while at the same time failing to maintain that information secure from intrusion and theft by hackers.

175. Under the common law doctrine of unjust enrichment, it is inequitable for Defendant to be permitted to retain the benefits it received, and is still receiving, without justification, from the use of Plaintiff's and Class Members' Private Information in an unfair and unconscionable manner. Defendant's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

176. The benefit conferred upon, received, and enjoyed by Defendant was not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendant to retain the benefit.

**COUNT V**
**INJUNCTIVE/DECLARATORY RELIEF**
**(On Behalf of Plaintiff and the Class)**

177. Plaintiff restates and realleges paragraphs 1 through 120, above as if fully set forth herein.

178. Defendant owes a duty of care to Plaintiff and Class Members requiring it to adequately secure Private Information.

179. Defendant still stores Plaintiff's and Class Members' Private Information.

180. Since the Data Breach, Defendant has announced no specific changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent similar incidents from occurring in the future.

181. Defendant has not satisfied its legal duties to Plaintiff and Class Members.

182. Actual harm has arisen in the wake of the Data Breach regarding Defendant's duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their Private Information, and Defendant's failure to address the security failings that led to that exposure.

183. Plaintiff, therefore, seeks a declaration: (a) that Defendant's existing security measures do not comply with its duties of care to provide adequate security; and (b) that to comply with its duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

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

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

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

d. ordering that Defendant segment Private Information by, among other things, creating firewalls and access controls so that if one area of Defendant's system is compromised, hackers cannot gain access to other portions of Defendant's system;

e. ordering that Defendant purge, delete, and destroy in a reasonably secure manner Private Information not necessary for its provision of services;

f. ordering that Defendant conduct regular computer system scanning and security checks; and

g. ordering that Defendant 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

## PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the class, respectfully requests that the Court enter judgment in Plaintiff's favor and against Defendant as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, nominal damages and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of himself and the Class, seeks appropriate injunctive relief designed to prevent Defendant from experiencing another data breach by adopting and implementing best data security practices to safeguard Private Information and to provide or extend credit monitoring services and similar services to protect against all types of identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

## JURY TRIAL DEMAND

Plaintiff demands a trial by jury of all claims herein so triable.

Dated: March 19, 2026.

Respectfully submitted,

*/s/ Christina Xenides*

Christina Xenides
**SIRI & GLIMSTAD LLP**
1005 Congress Avenue, Ste 925-C36
Austin, TX 78701
Tel: (512) 265-5622

E: cxenides@sirillp.com

Kenneth Grunfeld (*pro hac vice forthcoming*)
**KOPELOWITZ OSTROW P.A.**
One West Law Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tel: (954) 332-4200
E: grunfeld@kolawyers.com

*Counsel for Plaintiff and the Proposed Class*

# ClassAction.org



---