IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF WEST VIRGINIA

CRYSTAL ORTNER, individually, and on behalf of all others similarly situated,

Plaintiff,

v.

FAIRMONT FEDERAL CREDIT UNION,

Defendant.

Case No. 1:25-cv-98 Kleeh

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Crystal Ortner ("Plaintiff"), individually and on behalf of all other similarly situated individuals (the "Class" or "Class Members," as defined below), by and through her undersigned counsel, file this Class Action Complaint against Fairmont Federal Credit Union ("FFCU" or "Defendant") and allege the following based on personal knowledge of facts, upon information and belief, and based on the investigation of her counsel as to all other matters.

I. NATURE OF THE ACTION

1. Plaintiff brings this class action lawsuit against FFCU for its failure to protect and safeguard Plaintiff's and the Class's highly sensitive personally identifiable information ("PII"). As a result of FFCU's negligence and insufficient data security, a cybercriminal ransomware group easily infiltrated Defendant's inadequately protected network and stole the PII of Plaintiff and approximately 187,038 Class Members (the "Data Breach" or "Breach"). Now, Plaintiff's and the Class's PII is in the hands of cybercriminals who will undoubtedly use their PII for nefarious purposes for the rest of their lives.[1]

[1] OFFICE OF THE MAINE ATTORNEY GENERAL, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/75c92a2c-3791-47c6-84f7-87b34fab952d.html (last visited Sept. 22, 2025).

2. FFCU is a federally chartered financial institution providing banking services to individuals and business in West Virginia.[2]

3. According to information and belief, Plaintiff and Class Members are current or former customers for FFCU.

4. Plaintiff and the Class provided their PII to FFCU to receive financial and banking services.

5. Despite FFCU collecting and storing the highly confidential PII of Plaintiff and Class Members on its systems, FFCU failed to implement rudimentary data security measures, culminating in a massive and preventable data breach.

6. According to FFCU on January 23, 2024, it became aware of suspicious activity on its systems.[3]

7. After an investigation, FFCU determined that an unknown actor "accessed and/or acquired" files containing Plaintiff's and the Class's PII.[4]

8. The types of PII stolen in the Data Breach included names, telephone numbers, e-mail addresses, Date of Birth, Social Security number, account number and/or member ID number, financial institution name, Credit/Debit Card Number, and expiration date (collectively, "Private Information").[5]

9. Due to Defendant's negligence, cybercriminals have stolen and obtained everything they need to commit identity theft and wreak havoc on the financial and personal lives of thousands of individuals.

[2] https://www.fairmontfcu.com/about-us/about-fairmont-fcu.html (last visited Sept. 22, 2025).
[3] *See* Exhibit A, *Notice of Data Security Event*, attached hereto.
[4] *Id*.
[5] *Id*.

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

11. In sum, Plaintiff and the Class face an imminent risk of fraud and identity theft for the rest of their lives because (i) FFCU failed to protect Plaintiff's and the Class's Private Information, allowing a massive and preventable Data Breach to occur; (ii) the cybercriminals who perpetrated the Breach now are in possession of Private Information that they will post on the dark web (if they have not already); (iii) FFCU failed to provide any assurance that it paid a ransom to prevent Plaintiff's and the Class's Private Information from being released on the dark web; and (iv) FFCU offered credit monitoring to Plaintiff and the Class, an offer it need not make if no Private Information was stolen and at risk of misuse.

12. Plaintiff brings this action individually and on behalf of the Class, seeking compensatory damages, punitive damages, nominal damages, restitution, and injunctive and declaratory relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

II. THE PARTIES

13. Plaintiff Crystal Ortner is an adult individual who, at all relevant times, was a

resident and citizen of Fairmont, West Virginia.

14. Plaintiff Ortner received a notice letter from Defendant advising her that her Social Security number, account number and/or member ID, financial institution name, Credit/Debit Card Number and Expiration date were accessed and acquired during the Data Breach.

15. Defendant Fairmont Federal Credit Union is headquartered in Fairmont, West Virginia with its principal place of business located at 2 The Credit Union Way, Fairmont, West Virginia 26554.

III. JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than one hundred putative Class Members, and minimal diversity exists because many putative Class Members are citizens of a different state than Defendant, including Plaintiff.

17. This Court has personal jurisdiction over Defendant because Defendant is registered to do business in the State of West Virginia; has its principal place of business in this District; conducts substantial business in this District through its headquarters, offices, and affiliates; engaged in the conduct at issue here in this District; and/or otherwise has substantial contacts with this District and purposely availed itself to the Courts in this District.

18. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District.

IV. FACTUAL ALLEGATIONS

A. Defendant's Business and the Collection of Plaintiff's and the Class's Private Information.

19. FFCU is a not-for-profit organization, controlled, owned, and operated by the members.[6] It has 9 regional branches with over 120 employees and nearly $475,000,000 in assets.[7]

20. FFCU offers its customers Checking accounts via third-party vendor Kasasa; home mortgage loans; and individual retirement account services.[8]

21. FFCU was organized in 1939 and has grown to service anyone living or working in Marion, Monongalia, Preston, Harrison, and Taylor counties.

22. In the ordinary course of business, FFCU receives the Private Information from individuals, such as Plaintiff and the Class, from those who utilize FCCU banking and financial services.

23. FFCU obtains, collects, uses, and derives a benefit from the Private Information of Plaintiff's and Class Members. FFCU uses the Private Information it collects to provide services, making a profit therefrom. FFCU would not be able to obtain revenue if not for the acceptance and use of Plaintiff's and the Class's Private Information.

24. By collecting Plaintiff's and the Class's Private Information, FFCU assumed legal and equitable duties to Plaintiff and the Class to protect and safeguard their Private Information from unauthorized access and intrusion.

25. Under information and belief, FFCU provides Plaintiff and Class Members a copy of the privacy policy prior to providing banking and financial services.

---

[6] *https://www.fairmontfcu.com/about-us/about-fairmont-fcu.html*(last visited Sept. 22, 2025).
[7] *Id*.
[8] *Id.*

26. FFCU's assurances of maintaining high standards of cybersecurity make it evident that FFCU recognized it had a duty to use reasonable measures to protect the PII that it collected and maintained.

27. FFCU violated its own statements and failed to adopt reasonable and appropriate security practices and procedures including administrative, physical security, and technical controls to safeguard Plaintiff's and the Class's Private Information.

28. As a result, Plaintiff's and Class Members' Private Information was **accessed and stolen** from FFCU's inadequately secured data systems in a massive and preventable Data Breach.

B. FFCU's Massive and Preventable Data Breach.

29. FFCU provided the following information about the Data Breach in a letter of notice sent to Plaintiff and Class Members:

> **What Happened?**
> On or about January 23, 2024, we became aware that we had experienced a data security incident.
>
> **What Information Was Involved?**
> After an extensive investigation, we concluded on or about August 17, 2025 that one or more of the files accessed and/or acquired by the unauthorized party between September 30, 2023 and October 18, 2023 contain your full nume, telephone number, e-mail address, Date of Birth, Social Security number, account number and/or member ID number, financial institution name, Credit/Debit Card Number, and expiration Date.

30. Despite discovering the Data Breach on January 23, 2024, FFCU did not begin notifying individuals of the Data Breach until September 2025—approximately one and half (1.5) years later.

31. FFCU has made no assurances that it paid the ransom demand, therefore, there is no doubt that Plaintiff's and the Class's Private Information was released on the dark web.

32. Even if FFCU did pay the ransom demand, there is no reason why Plaintiff and the

Class should believe a cybercriminal group will suddenly choose to do the "right thing" and delete their Private Information.

33. "One of the biggest issues with paying a ransom is that you're gambling that hackers will keep to their word and restore systems. Unfortunately, when you're dealing with criminals, there's no guarantee. In fact, it's estimated that as many as 92 percent of firms fail to recover all of their data, with nearly a third losing at least half. If the hackers have successfully exfiltrated data as part of their attack, there's also no way of knowing what they'll do with this, even if a ransom is paid. Many cybergangs make additional revenue by selling the data on the dark web, especially if it contains valuable intellectual property or customer data."[9]

34. In recognition of the severity of the Data Breach, and the imminent risk of harm Plaintiff and the Class face, FFCU provided temporary credit monitoring and identity theft protection services. Such an offering is inadequate and will not prevent identity theft but will only alert Data Breach victims once identity theft has already occurred.

35. All in all, FFCU failed to take the necessary precautions required to safeguard and protect Plaintiff's and Class Members' PII from unauthorized access and exploitation.

36. Defendant's actions represent a flagrant disregard of the rights of Plaintiff and the Class, both as to privacy and property.

C. Cybercriminals Have Used and Will Continue to Use Plaintiff's and the Class's Private Information to Defraud Them.

37. Private Information is of great value to hackers and cybercriminals, and the data stolen in the Data Breach can and will be used in a variety of ways by criminals to exploit Plaintiff and the Class Members and to profit off their misfortune.

[9] Brenda Robb, *Should You Pay a Ransomware Demand?*, BLACKFOG (Feb. 28, 2024) https://www.blackfog.com/should-you-pay-a-ransomware-demand/ (last visited Sept. 22, 2025).

38. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[10]

39. For example, with the Private Information stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[11] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and the Class Members.

40. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number.** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[12]

(Emphasis added).

41. Private Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.[13]

---

[10] *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[11] *See, e.g.*, Christine DiGangi, *What Can You Do with a Stolen Social Security Number*, CREDIT.COM (June 29, 2020), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[12] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[13] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, available at https://www.gao.gov/products/gao-07-737.

42. This was a financially motivated Breach, as the only reason cybercriminals go through the trouble of running targeted cyberattacks against companies like FFCU is to get ransom money and/or information that they can monetize by selling on the dark web for use in the kinds of criminal activity described herein.

43. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[14]

44. "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[15]

45. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if hackers get access to PII, ***they will use it***.[16]

46. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n 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.[17]

[14] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web* (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.
[15] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.
[16] Ari Lazarus, *How fast will identity thieves use stolen info?*, MILITARY CONSUMER (May 24, 2017), https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info.
[17] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,* GAO (July 5, 2007), available at https://www.gao.gov/products/gao-07-737.

47. For instance, with a stolen social security number, which is part of the Private Information compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[18]

48. With this Data Breach, identity thieves have already started to prey on the FFCU Data Breach victims, and we can anticipate that this will continue.

49. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[19]

50. Defendant's limited offer of one (1) year of identity monitoring to Plaintiff and the Class is woefully inadequate and will not fully protect Plaintiff from the damages and harm caused by its failures.

51. The full scope of the harm has yet to be realized. 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.

52. Once the twelve (12) months have expired, Plaintiff and Class Members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives due to FFCU's gross negligence.

53. Furthermore, identity monitoring only alerts someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's

[18] *See, e.g.*, Christine DiGangi, *What Can You Do with a Stolen Social Security Number*, CREDIT.COM (June 29, 2020), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.
[19] *Guide for Assisting Identity Theft Victims*, FEDERAL TRADE COMMISSION (Sept. 2013), *available at* https://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf.

PII)—it does not prevent identity theft.[20] Nor can an identity monitoring service remove personal information from the dark web.[21]

54. "The people who trade in stolen personal information [on the dark web] won't cooperate with an identity theft service or anyone else, so it's impossible to get the information removed, stop its sale, or prevent someone who buys it from using it."[22]

55. As a direct and proximate result of the Data Breach, Plaintiff and the Class have been damaged and have been placed at an imminent, immediate, and continuing increased risk of harm from continued fraud and identity theft. Plaintiff and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

56. Even more seriously is the identity restoration that Plaintiff and other Class Members must go through, which can include spending countless hours filing police reports, filling out IRS forms, Federal Trade Commission checklists, Department of Motor Vehicle driver's license replacement applications, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps Plaintiff and the Class must take.

57. Plaintiff and the Class have or will experience the following concrete and particularized harms for which they are entitled to compensation, including:

a. Theft of their Private Information;

---

[20] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017, 9:00 AM), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html.
[21] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know.
[22] *Id.*

b. Actual identity theft;

c. Trespass, damage to, and theft of their personal property including Private Information;

d. Improper disclosure of their Private Information;

e. 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;

f. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their Private Information;

g. Ascertainable losses in the form of time taken to respond to identity theft and attempt to restore identity, including lost opportunities and lost wages from uncompensated time off from work;

h. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

i. Ascertainable losses in the form of deprivation of the value of Plaintiff's and Class Members' Private Information for which there is a well-established and quantifiable national and international market;

j. The loss of use of and access to their credit, accounts, and/or funds;

k. Damage to their credit due to fraudulent use of their Private Information; and/or

l. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

58. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which remains in the possession of Defendant, is protected from further

breaches by the implementation of industry standard security measures and safeguards. Defendant has shown itself wholly incapable of protecting Plaintiff's and the Class's Private Information.

59. Plaintiff and Class Members also have an interest in ensuring that their Private Information that was provided to FFCU is removed from all FFCU servers, systems, and files.

60. Defendant itself acknowledged the harm caused by the Data Breach because it offered Plaintiff and Class Members woefully inadequate identity theft repair and monitoring services. The identity theft and repair and monitoring offered is, however, inadequate to protect Plaintiff and Class Members from a lifetime of identity theft risk.

61. Defendant further acknowledged that the Data Breach would cause inconvenience to affected individuals and that financial harm would likely occur because it advised individuals to enroll in credit monitoring, place a fraud alert/security freeze on credit files, and obtain a free credit report.

62. At FFCU's suggestion, Plaintiff and the Class are desperately trying to mitigate the damage that FFCU has caused them.

63. Given the kind of Private Information FFCU made accessible to hackers, however, Plaintiff and the Class are certain to incur additional damages. Because identity thieves have their PII, Plaintiff and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[23]

64. None of this should have happened because the Data Breach was entirely preventable.

[23] *What happens if I change my Social Security number*, LEXINGTON LAW (Aug. 10, 2022), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

D. Defendant was Aware of the Risk of Cyberattacks.

65. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of the biggest cybersecurity breaches: Target,[24] Yahoo,[25] Marriott International,[26] Chipotle, Chili's, Arby's,[27] and others.[28]

66. Further, there has been a 34% increase in attackers exploiting vulnerabilities to gain initial access and cause security breaches in 2025.[29]

67. According to the Verizon 2025 Data Breach Investigation Report, Executive Summary, the financial and insurance industry has suffered 3,336 incidents, with 927 confirmed data disclosure breaches.[30]

68. FFCU should certainly have been aware, and indeed was aware, that it was at risk of a data breach that could expose the Private Information that it collected and maintained.

69. FFCU was clearly aware of the risks it was taking and the harm that could result from inadequate data security but threw caution to the wind.

---

[24] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

[25] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

[26] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/ (last visited Oct. 9, 2023).

[27] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018, 12:58 PM), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.

[28] *See, e.g.*, Michael Hill and Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Nov. 8, 2022), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[29] Verizon 2025 Data Breach Report, available at: https://www.verizon.com/business/resources/reports/dbir/

[30] *Id*.

E. FFCU Could Have Prevented the Data Breach.

70. Data breaches are preventable.[31] 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 solutions."[32] he 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 . . . ."[33]

71. "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*."[34]

72. In a data breach like this, many failures laid the groundwork for the Breach.

73. The FTC has published guidelines that establish reasonable data security practices for businesses.

74. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[35]

75. The FTC guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed;

---

[31] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012), available at https://lawcat.berkeley.edu/record/394088.
[32] *Id.* at 17.
[33] *Id.* at 28.
[34] *Id.*
[35] *Protecting Personal Information: A Guide for Business*, FTC, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems.

76. The FTC guidelines also recommend that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

77. According to information and belief, FFCU failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines.

78. Upon information and belief, FFCU also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity readiness.

79. 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."[36]

80. To prevent and detect cyberattacks Defendant could and should have implemented, as recommended by the Federal Bureau of Investigation, 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.

[36] *See* 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.

- 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.
- 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.[37]

81. Further, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….
- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the

[37] *Id.* at 3–4.

website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….
- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[38]

82. In addition, 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

[38] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), available at https://www.cisa.gov/news-events/news/protecting-against-ransomware.

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

- **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].[39]

83. Given that Defendant was storing the Private Information of thousands of individuals, Defendant could have and should have implemented all of the above measures to prevent and detect data breaches.

84. Specifically, among other failures, FFCU had far too much confidential unencrypted information held on its systems. Such Private Information should have been segregated into an encrypted system.[40]

85. Moreover, it is a well-established industry standard practice for a business to dispose of confidential Private Information once it is no longer needed.

86. The FTC, among others, has repeatedly emphasized the importance of disposing unnecessary Private Information, saying simply: "Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it.

[39] *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/.

[40] *See, e.g.,* Adnan Raja, *How to Safeguard Your Business Data with Encryption*, FORTRA (Aug. 14, 2018), https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption.

If it's not on your system, it can't be stolen by hackers."[41] FFCU, rather than following this basic standard of care, kept thousands of people's unencrypted Private Information indefinitely.

87. In sum, the Data Breach could have readily been prevented through the use of industry standard network segmentation and encryption of all Private Information.

88. Further, the scope of the Data Breach could have been dramatically reduced had FFCU utilized proper record retention and destruction practices.

V. DEFENDANT'S BREACH

89. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and its data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to train employees in the proper handling of emails containing malicious software, and to and maintain adequate email security practices;

e. Failing to put into place proper procedures, software settings, and data security software protections to adequately protect against a blunt force intrusion;

f. Failing to comply with FTC guidelines for cybersecurity, in violation of Section *5* of the FTC Act; and

g. Failing to adhere to industry standards for cybersecurity.

90. As the result of computer systems needing security upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, and

[41] *Protecting Personal Information: A Guide for Business*, FTC, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf, at p. 6.

inadequately trained employees who opened files containing the ransomware virus, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

91. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft.

Because of Defendant's Failure to Safeguard Private Information, Plaintiff and the Class Members Have and Will Experience Substantial Harm in the Form of Risk of Continued Identity Theft.

92. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

93. The ramifications of Defendant's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes. According to experts, one out of four data breach notification recipients become a victim of identity fraud.

94. Because of Defendant's failures to prevent—and to timely detect—the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

95. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

96. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals often post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

97. It can take victims years to spot identity or PII theft, giving criminals plenty of time to milk that information for cash.

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

99. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

100. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and

sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII is being misused, and that such misuse is traceable to the Data Breach.

101. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims, and the numbers are only rising.

102. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good" Defendant did not rapidly report to Plaintiff and the Class that their PII had been stolen.

103. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

104. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

105. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and the Class

will need to remain vigilant against unauthorized data use for years or even decades to come.

106. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[42]

107. The FTC has also issued many guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires:

(1) encrypting information stored on computer networks;

(2) retaining payment card information only as long as necessary;

(3) properly disposing of personal information that is no longer needed;

(4) limiting administrative access to business systems;

(5) using industry-tested and accepted methods for securing data;

(6) monitoring activity on networks to uncover unapproved activity;

(7) verifying that privacy and security features function properly;

(8) testing for common vulnerabilities; and

(9) updating and patching third-party software.

108. According to the FTC, unauthorized PII disclosures ravage consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.[43] The

[42] Statement of FTC Commissioner Pamela Jones Harbour-Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited February 3, 2025).

[43] *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), *available at* https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen (last visited February 3, 2025).

FTC treats 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(a) of the FTC Act.

109. Defendant's failure to properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff's and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

VI. PLAINTIFF'S EXPERIENCE

110. Plaintiff Ortner is a customer and member of FFCU.

111. Plaintiff provided her Private Information to Defendant as a condition of her membership with Defendant, which was held on Defendant's computer system and maintained by Defendant.

112. Plaintiff reasonably understood and expected that Defendant would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff would not have allowed Defendant, or anyone in Defendant's position, to maintain her Private Information if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

113. Plaintiff received a Notice Letter dated September 11, 2025, from Defendant informing her that her Private information had been viewed and copied by an unauthorized actor.

114. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff faces, Defendant offered her a twelve-month subscription to a credit monitoring service. The Notice Letter Plaintiff received also cautioned her to remain vigilant against incidents of

identity theft and fraud by reviewing your account statements and monitoring your credit reports for suspicious activity.

115. Plaintiff greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

116. As a consequence of and following the Data Breach, Plaintiff has suffered spam emails and text messages suggesting that her Private Information is now in the hands of cybercriminals.

117. Once an individual's Private Information is for sale and access on the dark web, as Plaintiff's Private Information is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[44] On information and belief, Plaintiff's phone number was also compromised as a result of the Data Breach.

118. Plaintiff stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

119. To the best of Plaintiff's knowledge, her PII has not been compromised in a prior data breach.

120. As a result of the Data Breach, Plaintiff has spent hours researching the Data Breach, verifying the legitimacy of the Notice Letter, reviewing her bank accounts, monitoring her

[44] Ryan Toohil, *What do Hackers do with Stolen Information*, AURA, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited Mar. 21, 2025).

credit report, signing up for Defendant's abbreviated credit monitoring services, and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

121. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by Defendant's delay in noticing her of the fact that her Private Information was acquired by criminals as a result of the Data Breach.

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

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

124. Plaintiff has suffered injuries directly and proximately caused by the Data Breach, including: (i) theft of Plaintiff valuable Private Information; (ii) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's Private Information being placed in the hands of cybercriminals; (iii) damages to and/or diminution in value of Plaintiff's Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff's Private Information; and (v) continued risk to Plaintiff's Private

Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

VII. CLASS ACTION ALLEGATIONS

125. Plaintiff incorporates by reference all preceding paragraphs as if fully restated here.

126. Plaintiff brings this action against FFCU on behalf of themselves and all other individuals similarly situated under Federal Rule of Civil Procedure 23. Plaintiff asserts all claims on behalf of a nationwide class (the "Class") defined as follows:

> **All individuals who were sent a Notice Letter from FFCU and whose Private Information was accessed and/or acquired in the Data Breach.**

127. Excluded from the Class is Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

128. Plaintiff reserves the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

129. Plaintiff anticipates the issuance of notice setting forth the subject and nature of the instant action to the proposed Class. Upon information and belief, Defendant's own business records or electronic media can be utilized for the notice process.

130. The proposed Class meets the requirements of Federal Rule of Civil Procedure 23.

131. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. The Class is comprised of over 187,038 individuals.

132. **Typicality:** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through FFCU's uniform misconduct. FFCU's inadequate data security gave rise to Plaintiff's claims and are identical to those that give rise to the claims of every other Class Member because Plaintiff and each member of the Class had their sensitive Private Information compromised in the same way by the same conduct of FFCU.

133. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and their counsel.

134. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress FFCU's wrongdoing. Even if Class Members could afford such individual litigation, the Court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

135. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions

predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiff's and the Class's Private Information;

c. Whether Defendant owed a duty to Plaintiff and the Class to adequately protect their Private Information, and whether it breached this duty;

d. Whether Defendant breached its duties to Plaintiff and the Class;

e. Whether Defendant failed to provide adequate cyber security;

f. Whether Defendant knew or should have known that its computer and network security systems were vulnerable to cyberattacks;

g. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its company network;

h. Whether Defendant was negligent in permitting unencrypted Private Information off vast numbers of individuals to be stored within its network;

i. Whether Defendant was negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breach;

j. Whether Defendant breached implied contractual duties to Plaintiff and the Class to use reasonable care in protecting their Private Information;

k. 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 the Class;

l. Whether Defendant continues to breach duties to Plaintiff and the Class;

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

n. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief; and

o. Whether Defendant's actions alleged herein constitute gross negligence, and whether Plaintiff and Class Members are entitled to punitive damages.

VIII. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

136. Plaintiff re-alleges and incorporate the above allegations as if fully set forth herein.

137. FFCU solicited, gathered, and stored the Private Information of Plaintiff and Class Members.

138. Upon accepting and storing the Private Information of Plaintiff and Class Members on its computer systems and networks, Defendant undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information of Plaintiff and the Class from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

139. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information was wrongfully disclosed. Plaintiff and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class Members had no ability to protect their Private Information that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiff and the Class.

140. Because of this special relationship, Defendant required Plaintiff and Class Members to provide their Private Information, including names, Social Security numbers, and other Private Information.

141. Implied in these exchanges was a promise by Defendant to ensure that the Private Information of Plaintiff and Class Members in its possession was only used for the provided purpose and that Defendant would destroy any Private Information that it was not required to maintain.

142. As part of this special relationship, Defendant had a duty to perform with skill, care, and reasonable expedience and faithfulness.

143. Through Defendant's acts and omissions, including Defendant's failure to provide adequate data security, its failure to protect Plaintiff's and Class Members' Private Information from being foreseeably accessed, and its improper retention of Private Information it was not required to maintain, Defendant negligently failed to observe and perform its duty.

144. Plaintiff and Class Members did not receive the benefit of the bargain with Defendant, because providing their Private Information was in exchange for Defendant's implied agreement to secure and keep it safe and to delete it once no longer required.

145. Defendant was aware of the fact that cybercriminals routinely target large entities such as Defendant through cyberattacks in an attempt to steal customer Private Information. In other words, Defendant knew of a foreseeable risk to its data security systems but failed to implement reasonable security measures.

146. Defendant owed Plaintiff and the Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing Private Information, including taking action to reasonably safeguard

or delete such data and providing notification to Plaintiff and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

147. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

148. Defendant had duties to protect and safeguard the Private Information of Plaintiff and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive Private Information. Additional duties that Defendant owed Plaintiff, and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiff's and Class Members' Private Information was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiff's and Class Members' Private Information in its possession by using reasonable and adequate security procedures and systems;

c. To implement processes to quickly detect a data breach, security incident, or intrusion involving its networks and servers; and

d. To promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their Private Information.

149. Plaintiff and the Class were the intended beneficiaries of Defendant's duties, creating a special relationship between them and Defendant. Defendant was in a position to ensure

that its systems were sufficient to protect the Private Information that Plaintiff and the Class had entrusted to it.

150. Plaintiff's injuries and damages, as described herein, are a reasonably certain consequence of Defendant's negligence and breach of its duties.

151. Defendant breached its duties of care by failing to adequately protect Plaintiff's and Class Members' Private Information. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, and protecting the Private Information in its possession;

b. Failing to protect the Private Information in its possession using reasonable and adequate security procedures and systems;

c. Failing to consistently enforce security policies aimed at protecting Plaintiff and the Class's Private Information;

d. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

e. Failing to promptly notify Plaintiff and Class Members of the Data Breach that affected their Private Information.

152. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent considering the foreseeable risks and known threats.

153. As a direct and proximate result of Defendant's negligent conduct, including but not limited to its failure to implement and maintain reasonable data security practices and procedures as described above, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

154. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Private Information of Plaintiff and Class Members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiff and Class Members while it was within Defendant's possession and control.

155. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendant prevented Plaintiff and Class Members from taking meaningful, proactive steps to securing their Private Information and mitigating damages.

156. Plaintiff and Class Members could have taken actions earlier had they been timely notified of the Data Breach.

157. Plaintiff and Class Members could have enrolled in credit monitoring, could have instituted credit freezes, and could have changed their passwords, among other things, had they been alerted to the Data Breach more quickly.

158. Plaintiff and Class Members have suffered harm from the delay in notifying them of the Data Breach.

159. As a direct and proximate cause of Defendant's conduct, including but not limited to its failure to implement and maintain reasonable security practices and procedures, Plaintiff and Class Members have suffered, as Plaintiff have, and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their Private Information is used; (ii) the publication and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information, including the need for substantial credit monitoring and identity protection services for an extended period of time; (iv) lost opportunity

costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual 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 identity theft; (v) costs associated with placing freezes on credit reports and password protections; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of customers in its continued possession; and (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Private Information for the rest of their lives. Thus, Plaintiff and the Class are entitled to damages in an amount to be proven at trial.

160. The damages Plaintiff and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's negligent conduct.

161. Plaintiff and the Class have suffered injury and are entitled to actual and punitive damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

162. Plaintiff re-allege and incorporate the above allegations as if fully set forth herein.

163. Plaintiff and Class Members were required to provide their Private Information to Defendant as part of the process of obtaining employment and/or services from Defendant.

164. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

165. Defendant accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing employment and/or services to Plaintiff and Class Members.

166. Plaintiff and the Class entrusted their Private Information to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

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

168. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide Private Information, was the latter's obligation to: (i) use such Private Information for business purposes only; (ii) take reasonable steps to safeguard that Private Information; (iii) prevent unauthorized disclosures of the Private Information; (iv) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information; (v) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses; and (vi) retain the Private Information only under conditions that kept such information secure and confidential.

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

170. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

171. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' Private Information would remain protected.

172. Plaintiff and Class Members provided labor and/or paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

173. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

174. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

175. Every contract has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

176. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

177. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

178. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Private Information, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of Private Information and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

179. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members sustained damages, including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

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

181. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

THIRRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

182. Plaintiff re-allege and incorporate the above allegations as if fully set forth herein.

183. Plaintiff alleged this claim in the alternative to their breach of contract claim.

184. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiff's retained data and commercialized and used Plaintiff's and Class Members' Private Information for business purposes.

185. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including: (i) payments on behalf of or for the benefit of Plaintiff and Class Members; and (ii) revenue obtained from Plaintiff and Class Members labor.

186. As such, a portion of the payments made for the benefit of or on behalf of Plaintiff and Class Members 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.

187. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

188. Defendant acquired the Private Information through inequitable means as it failed to disclose the inadequate data security practices previously alleged. If Plaintiff and Class

Members had known that Defendant would not fund adequate data security practices, procedures, and protocols to sufficiently monitor, supervise, and secure their Private Information, they would not have entrusted their Private Information to Defendant.

189. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to their own benefit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

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

191. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

192. As a direct and proximate result of Defendant's conduct, Plaintiff and other Class Members, have suffered actual harm in the form of experiencing specific acts of fraudulent activity and other attempts of fraud that required Plaintiff's efforts to prevent from succeeding.

193. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the Class are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by Defendant and all other relief allowed by law.

IX. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class described above seeks the following relief:

a. For an Order certifying this action as a class action, defining the Class as requested herein, appointing Plaintiff and her counsel to represent the Class, and finding that Plaintiff is a proper representative of the Class requested herein;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein relating to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c. For equitable relief compelling Defendant to use appropriate methods and policies related to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d. For an order directing Defendant to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;

e. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

f. For an award of punitive damages, as allowable by law;

g. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

h. Pre- and post-judgment interest on any amounts awarded; and

i. Any other relief that this court may deem just and proper.

X. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all appropriate issues raised in this Class Action Complaint.

Date: September 24, 2025

Respectfully Submitted,

*/s/*Hoyt Glazer
Hoyt Glazer**
West Virginia Bar No. 6479
hoyt@gsalaw-wv.com
GLAZER SAAD ANDERSON L.C.
320 Ninth Street, Suite B
Huntington, West Virginia 25701
Phone: (304) 522-4149
Fax: (800) 879-7248

Leigh S. Montgomery*
Texas Bar No. 24052214
lmontgomery@eksm.com
service@eksm.com
EKSM, LLP
4200 Montrose Blvd., Suite 200
Houston, Texas 77006
Phone: (888) 350-3931
Fax: (888) 276-3455

COUNSEL FOR PLAINTIFF AND THE PUTATIVE CLASS
(* denotes *pro hac vice* forthcoming)
(** local counsel)