

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WISCONSIN**

MATTHEW THOMSON, on behalf of himself
and all others similarly situated,

Plaintiff,

v.

COMMUNITY FIRST CREDIT UNION,

Defendant.

CLASS ACTION COMPLAINT

DEMAND FOR A JURY TRIAL

Plaintiff Matthew Thomson (“Plaintiff”) brings this Class Action Complaint (“Complaint”) against Community First Credit Union (“CFCU” or “Defendant”) as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels’ investigation, and upon information and belief as to all other matters, as follows:

SUMMARY OF ACTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard sensitive information of its customers.
2. Defendant is a Wisconsin-based credit union.
3. Plaintiff’s and Class Members’ sensitive personal information—which they entrusted to Defendant on the mutual understanding that Defendant would protect it against disclosure—was targeted, compromised, and unlawfully accessed due to the Data Breach.
4. CFCU collected and maintained certain personally identifiable information and protected health information of Plaintiff and the putative Class Members (defined below), who are (or were) customers at Defendant.

5. The PII compromised in the Data Breach included Plaintiff's and Class Members' full names, account numbers, and Social Security numbers ("personally identifiable information" or "PII").

6. The PII compromised in the Data Breach was exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals who target PII for its value to identity thieves.

7. As a result of the Data Breach, Plaintiff and Class Members suffered concrete injuries in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (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) Plaintiff experiencing fraudulent charges to his Chase credit card, totaling approximately \$2,000, in or about May 2024; (viii) Plaintiff's PII being disseminated on the dark web, according to Chase; (ix) actual misuse of their PII consisting of an increase in spam calls, texts, and/or emails; statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their PII, 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 PII.

8. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its customers' PII from a foreseeable and preventable cyber-attack.

9. Moreover, upon information and belief, Defendant was targeted for a cyber-attack due to its status as a financial institution that collects and maintains highly valuable PII on its systems.

10. Defendant maintained, used, and shared the PII in a reckless manner. In particular, the PII was used and transmitted by Defendant in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

11. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

12. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct because the PII that Defendant collected and maintained has been accessed and acquired by data thieves.

13. Armed with the PII accessed in the Data Breach, data thieves have already engaged in identity theft and fraud and can in the future commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

14. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

15. Plaintiff and Class Members may also incur out of pocket costs, *e.g.*, for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

16. Plaintiff brings this class action lawsuit on behalf all those similarly situated to address Defendant's inadequate safeguarding of Class Members' PII that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

17. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose PII was accessed during the Data Breach.

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

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including Plaintiff, is a citizen of a state different from Defendant.

20. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

21. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

PARTIES

22. Plaintiff Matthew Thomson is a resident and citizen of Novato, California.

23. Defendant is a member owned non-profit credit union with its principal place of business located in Appleton, Wisconsin.

FACTUAL ALLEGATIONS

Defendant's Business

24. Defendant is a Wisconsin-based credit union.

25. Plaintiff and Class Members are current and former customers of Defendant.

26. In the course of their relationship, customers, including Plaintiff and Class Members, provided Defendant with at least the following: names, Social Security numbers, and other sensitive information.

27. Upon information and belief, in the course of collecting PII from its customers, including Plaintiff, Defendant promised to provide confidentiality and adequate security for the data it collected from its customers through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

28. Indeed, Defendant provides on its website that:

CFCU will restrict access to non-public personal information about current, prospective and former members to CFCU employees who have a specific business purpose in utilizing the data. CFCU Management will ensure employees are trained in the importance of preserving confidentiality and member privacy.

It is the policy of CFCU to comply with the provisions of both the Gramm-Leach-Bliley Act and the NCUA Privacy Regulations.¹

¹ <https://www.communityfirstcu.org/privacy-accessibility>

The Data Breach

29. On or about May 3, 2024, Defendant began sending Plaintiff and other Data Breach victims an untitled letter (the "Notice Letter"), informing them that:

What Happened?

Between September 6, 2023 and September 7, 2023, an unauthorized third party obtained access to the contents of one employee's e-mail account in an attempt to commit financial fraud against the company. The attempted financial fraud was promptly identified and blocked. When we discovered the suspicious activity, our technology team acted quickly to block any further attempts to access the account and further secure our systems. We also engaged third-party cybersecurity experts to conduct an investigation to determine the full nature and scope of the event.

At the conclusion of the initial investigation, we determined that an unauthorized actor potentially viewed certain information contained within the affected account. With the results of the investigation, we began a comprehensive review of the affected employee's email account. Our comprehensive investigation and review recently concluded on April 16, 2024 and determined that your personal information was included within the data that may have been viewed by the unauthorized actor. We wanted to notify you of the incident out of an abundance of caution and provide you information on steps you can take to protect yourself against possible misuse of the information.

What Information Was Involved.

The information involved in the incident included your first and last name and your Social Security number, and account number.²

30. Omitted from the Notice Letter were the date that Defendant detected the Data Breach, the identity of the cybercriminals who perpetuated the cyberattack, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

² The "Notice Letter". A sample copy is available at <https://oag.ca.gov/ecrime/databreach/reports/sb24-584828>

31. This “disclosure” amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach’s critical facts. Without these details, Plaintiff’s and Class Members’ ability to mitigate the harms resulting from the Data Breach is severely diminished.

32. Despite Defendant’s intentional opacity about the root cause of this incident, several facts may be gleaned from the Notice Letter, including: a) that this Data Breach was the work of cybercriminals; b) that 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’ Social Security numbers for download and theft.

33. In the context of notice of data breach letters of this type, Defendant’s use of the phrase “may have been viewed” is misleading lawyer language. Companies only send notice letters because data breach notification laws require them to do so. And such letters are only sent to those persons who Defendant itself has a reasonable belief that such personal information was accessed or acquired by an unauthorized individual or entity. Defendant cannot hide behind legalese – by sending a notice of data breach letter to Plaintiff and Class Members, it admits that Defendant itself has a reasonable belief that Plaintiff’s and Class Members’ names, Social Security numbers, and account information was accessed or acquired by an unknown actor – aka cybercriminals.

34. Moreover, in its Notice Letter, Defendant failed to specify whether it undertook 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 or whether Defendant

was interested in hearing about misuse of their data or set up a mechanism for Class Members to report misuse of their data.

35. Defendant had obligations created by the FTC Act, GLBA, contract, common law, and industry standards to keep Plaintiff's and Class Members' PII confidential and to protect it from unauthorized access and disclosure.

36. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

37. The attacker accessed and acquired files Defendant shared with a third party containing unencrypted PII of Plaintiff and Class Members. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

38. Plaintiff has been informed by Chase that his PII has been disseminated on the dark web, and Plaintiff further believes that the PII 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 type.

Data Breaches Are Preventable

39. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

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

41. 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.”³

42. To prevent and detect cyber-attacks and/or ransomware 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.
- 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

³ 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>

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.⁴

43. 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

⁴ *Id.* at 3-4.

- 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].⁵

44. Given that Defendant was storing the PII of its current and former customers, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

45. 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 data thieves acquiring and accessing the PII of, upon information and belief, thousands to tens of thousands of individuals, including that of Plaintiff and Class Members.

Defendant Acquires, Collects, And Stores Its Customers' PII

46. Defendant acquires, collects, and stores a massive amount of PII on its current and former customers.

47. As a condition of obtaining services at Defendant, Defendant requires that its customers and other personnel entrust it with highly sensitive personal information.

48. By obtaining, collecting, and using Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

⁵ 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/>

49. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII and would not have entrusted it to Defendant absent a promise to safeguard that information.

50. Upon information and belief, in the course of collecting PII from its customers, including Plaintiff, Defendant promised to provide confidentiality and adequate security for their data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

51. Indeed, Defendant provides on its website that:

CFCU will restrict access to non-public personal information about current, prospective and former members to CFCU employees who have a specific business purpose in utilizing the data. CFCU Management will ensure employees are trained in the importance of preserving confidentiality and member privacy.

It is the policy of CFCU to comply with the provisions of both the Gramm-Leach-Bliley Act and the NCUA Privacy Regulations.⁶

52. Plaintiff and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Defendant Knew, Or Should Have Known, of the Risk Because Financial Institutions In Possession Of PII Are Particularly Susceptible To Cyber Attacks

53. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting financial institutions that collect and store PII, like Defendant, preceding the date of the breach.

54. Data breaches, including those perpetrated against financial institutions that store PII in their systems, have become widespread.

⁶ <https://www.communityfirstcu.org/privacy-accessibility>

55. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.⁷

56. In light of recent high profile data breaches at other industry leading companies, including T-Mobile, USA (37 million records, February-March 2023), 23andMe, Inc. (20 million records, October 2023), Wilton Reassurance Company (1.4 million records, June 2023), NCB Management Services, Inc. (1 million records, February 2023), Defendant knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

57. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals...because they often have lesser IT defenses and a high incentive to regain access to their data quickly."⁸

58. Additionally, as companies became more dependent on computer systems to run their business,⁹ *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.¹⁰

⁷ See <https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/>

⁸ https://www.law360.com/employee-protection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=employee-protection

⁹ <https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html>

¹⁰ <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022>

59. Defendant knew and understood unprotected or exposed PII in the custody of insurance companies, like Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access.

60. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

61. 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 PII.

62. 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 PII of Plaintiff and Class Members.

63. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

64. As a financial institution in custody of the PII of its customers, Defendant knew, or should have known, the importance of safeguarding PII entrusted to it by Plaintiff and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Value Of PII

65. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”¹¹ 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.”¹²

66. 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.¹³

67. For example, Personal Information can be sold at a price ranging from \$40 to \$200.¹⁴ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.¹⁵

68. Moreover, Social Security numbers, which were breached for some members of the Class, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

69. 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

¹¹ 17 C.F.R. § 248.201 (2013).

¹² *Id.*

¹³ *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/>

¹⁴ *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/>

¹⁵ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/>

accounts, credit cards, driving records, tax and employment histories and other private information increases.”¹⁶ Moreover, “[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains.”¹⁷

70. The Social Security Administration stresses that the loss of an individual’s Social Security number, as experienced by Plaintiff and some 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.¹⁸

71. In fact, “[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health.”¹⁹ “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.”²⁰

72. 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

¹⁶ See

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

¹⁷ *Id.*

¹⁸ Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf>

¹⁹ See <https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/>

²⁰ See <https://www.investopedia.com/terms/s/ssn.asp>

misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

73. 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.”²¹

74. 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 *4 (citations omitted) (S.D.N.Y. Mar. 8, 2021) (the court noted that Plaintiff’s 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.”)

²¹ 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>

75. Similarly, the California state government warns consumers that: “[o]riginally, your Social Security number (SSN) was a way for the government to track your earnings and pay you retirement benefits. But over the years, it has become much more than that. It is the key to a lot of your personal information. With your name and SSN, an identity thief could open new credit and bank accounts, rent an apartment, or even get a job.”²²

76. 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 and names.

77. 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

78. 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.

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

²² See <https://oag.ca.gov/idtheft/facts/your-ssn>

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>

[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

80. 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 PII.

Defendant Fails To Comply With FTC Guidelines

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

82. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies to correct any security problems.²⁵

83. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone

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

²⁵ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.²⁶

84. The FTC further recommends that companies not maintain PII longer than is 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.

85. 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 customer 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.

86. These FTC enforcement actions include actions against credit unions, like Defendant.

87. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

88. Defendant failed to properly implement basic data security practices.

²⁶ *Id.*

89. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to the PII of its customers or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

90. Upon information and belief, CFCU was at all times fully aware of its obligation to protect the PII of its customers, CFCU was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

Defendant Violated The Gramm-Leach-Bliley Act

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

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

93. Defendant collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Defendant were subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1, *et seq.*, and is subject to numerous rules and regulations promulgated on the GLBA statutes.

94. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing

regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 (“Regulation P”), with the final version becoming effective on October 28, 2014.

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

96. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be “clear and conspicuous.” 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. “Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.” 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must “accurately reflect[] [the financial institution’s] privacy policies and practices.” 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution’s security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided “so that each consumer can reasonably be expected to receive actual notice.” 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Defendant violated the Privacy Rule and Regulation P.

97. Defendant failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers’ PII and storing that PII on Defendant's network systems.

98. Defendant failed to adequately inform their customers that they were storing and/or sharing, or would store and/or share, the customers' PII on an insecure platform, accessible to unauthorized parties from the internet, and would do so after the customer relationship ended.

99. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4.

100. As alleged herein, Defendant violated the Safeguard Rule.

101. Defendant failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information.

102. Defendant violated the GLBA and its own policies and procedures by sharing the PII of Plaintiff and Class Members with a non-affiliated third party without providing Plaintiff and Class Members (a) an opt-out notice and (b) a reasonable opportunity to opt out of such disclosure.

Defendant Fails To Comply With Industry Standards

103. As noted above, experts studying cyber security routinely identify financial institutions in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

104. Several best practices have been identified that, at a minimum, should be implemented by financial institutions in possession of PII, like Defendant, including but not limited to: educating all employees; 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. CFCU failed to follow these industry best practices, including a failure to implement multi-factor authentication.

105. Other best cybersecurity practices that are standard for financial institutions 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 protection of physical security systems; protection against any possible communication system; training staff regarding critical points. CFCU failed to follow these cybersecurity best practices, including failure to train staff.

106. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

107. These foregoing frameworks are existing and applicable industry standards for financial institutions, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Common Injuries & Damages

108. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to their PII, 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 PII.

Data Breaches Increase Victims' Risk Of Identity Theft

109. As Plaintiff has already experienced, the unencrypted PII of Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

110. Unencrypted PII may also fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Simply put, unauthorized individuals can easily access the PII of Plaintiff and Class Members.

111. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

112. Plaintiff's and Class Members' PII is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

113. Due to the risk of one's Social Security number being exposed, state legislatures have passed laws in recognition of the risk: "[t]he social security number can be used as a tool to perpetuate fraud against a person and to acquire sensitive personal, financial, medical, and familial information, the release of which could cause great financial or personal harm to an individual. While the social security number was intended to be used solely for the administration of the federal Social Security System, over time this unique numeric identifier has been used extensively for identity verification purposes[.]"²⁷

114. Moreover, "SSNs have been central to the American identity infrastructure for years, being used as a key identifier[.] . . . U.S. banking processes have also had SSNs baked into their identification process for years. In fact, SSNs have been the gold standard for identifying and verifying the credit history of prospective customers."²⁸

115. "Despite the risk of fraud associated with the theft of Social Security numbers, just five of the nation's largest 25 banks have stopped using the numbers to verify a customer's identity

²⁷ See N.C. Gen. Stat. § 132-1.10(1).

²⁸ See <https://www.americanbanker.com/opinion/banks-need-to-stop-relying-on-social-security-numbers>

after the initial account setup[.]”²⁹ Accordingly, since Social Security numbers are frequently used to verify an individual’s identity after logging onto an account or attempting a transaction, “[h]aving access to your Social Security number may be enough to help a thief steal money from your bank account”³⁰

116. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of “Fullz” packages.³¹

117. With “Fullz” packages, 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 in order to assemble complete dossiers on individuals.

118. The development of “Fullz” packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff’s and Class Members’ 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

²⁹ See <https://archive.nytimes.com/bucks.blogs.nytimes.com/2013/03/20/just-5-banks-prohibit-use-of-social-security-numbers/>

³⁰ See <https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>

³¹ “Fullz” is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. See, e.g., Matthew Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), <https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-1>(<https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/>

that was exfiltrated in the Data Breach, criminals may still 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.

119. The existence and prevalence of “Fullz” packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like insurance information) of Plaintiff and the other Class Members.

120. Thus, even if certain information (such as insurance information) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package.

121. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss Of Time To Mitigate Risk Of Identity Theft & Fraud

122. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

123. Thus, due to the actual and imminent risk of identity theft, Defendant, in its Notice Letter instructs Plaintiff and Class Members to take the following measures to protect themselves: “remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.”³²

³² Notice Letter.

124. In addition, Defendant’s Notice letter includes five pages devoted “Other Important Information” that recommend Plaintiff and Class Members to partake in activities such as enrolling in credit monitoring services, obtaining credit reports, placing security freezes on their accounts, and contacting government agencies.³³

125. Defendant’s extensive suggestion of steps that Plaintiff and Class Members must take in order to protect themselves from identity theft and/or fraud demonstrates the significant time that Plaintiff and Class Members must undertake in response to the Data Breach. Plaintiff’s and Class Members’ time is highly valuable and irreplaceable, and accordingly, Plaintiff and Class Members suffered actual injury and damages in the form of lost time that they spent on mitigation activities in response to the Data Breach and at the direction of Defendant’s Notice Letter.

126. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach, changing passwords and resecuring their own computer networks, and monitoring their financial accounts for any unusual activity. Accordingly, the Data Breach has caused Plaintiff and Class Members to suffer actual injury in the form of lost time—which cannot be recaptured—spent on mitigation activities.

127. Plaintiff’s mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”³⁴

³³ *Id.*

³⁴ See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

128. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.³⁵

129. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."⁴

Diminution of Value of PII

130. PII is a valuable property right.³⁶ Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

131. Sensitive PII can sell for as much as \$363 per record according to the Infosec Institute.³⁷

³⁵ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps>

³⁶ See "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> ("GAO Report").

³⁷ See, e.g., John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

132. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly \$200 billion.³⁸

133. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.^{39,40}

134. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.⁴¹

135. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

136. At all relevant times, CFCU knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

137. The fraudulent activity resulting from the Data Breach may not come to light for years.

³⁸ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>

³⁹ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

⁴⁰ <https://datacoup.com/>

⁴¹ <https://digi.me/what-is-digime/>

138. 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 PII.

139. CFCU was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to, upon information and belief, thousands to tens of thousands of individuals detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

140. 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 PII of Plaintiff and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

141. Given the type of targeted attack in this case, sophisticated criminal activity, the type of PII involved, and Plaintiff's PII already being disseminated on the dark web, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –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.

142. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her PII 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.

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

144. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach.

Loss of Benefit of the Bargain

145. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant for services, Plaintiff and other reasonable consumers understood and expected that they were paying, in part, for service and necessary data security to protect the PII, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiff Matthew Thomson's Experience

146. Plaintiff is a current customer of Defendant.

147. As a condition of obtaining services from Defendant, he was required to provide his PII to Defendant, including his name, Social Security number, and other sensitive information.

148. At the time of the Data Breach—September 6, 2023 through September 7, 2023—Defendant maintained Plaintiff's PII in its system.

149. Plaintiff Thomson is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted his PII to Defendant had he known of Defendant's lax data security policies.

150. Plaintiff Matthew Thomson received the Notice Letter, by U.S. mail, directly from Defendant, dated May 3, 2024. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his name, account number, and Social Security number.

151. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, which instructs Plaintiff to "remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis[,]"⁴² Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, changing passwords and resecuring his own computer network, and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

152. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to his PII, 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 PII.

⁴² Notice Letter.

153. Plaintiff further suffered actual injury in the form of experiencing fraudulent charges to his Chase credit card, totaling approximately \$2000, in or about May 2024, which, upon information and belief, was caused by the Data Breach.

154. Plaintiff also suffered actual injury in the form of his PII being disseminated on the dark web, according to Chase, which, upon information and belief, was caused by the Data Breach

155. Plaintiff additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of his PII was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

156. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

157. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

158. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

159. Plaintiff Matthew Thomson has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

160. Plaintiff brings this class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

161. The Classes that Plaintiff seeks to represent is defined as follows:

Nationwide Class

All individuals residing in the United States whose PII was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Defendant in May 2024 (the "Class").

California Subclass

All individuals residing in the State of California whose PII was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Defendant in May 2024 (the "California Subclass").

162. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

163. Plaintiff reserves the right to amend the definitions of the Class and/or California Subclass or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

164. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. Although the precise number of individuals is

currently unknown to Plaintiff and exclusively in the possession of Defendant, upon information and belief, thousands of individuals were impacted. The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

165. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

- a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;
- b. Whether Defendant had respective duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendant had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;
- d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;
- e. Whether and when Defendant actually learned of the Data Breach;
- f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;
- g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

- h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;
- k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

166. Typicality: Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

167. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenges of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

168. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages he has suffered are typical of

other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intend to prosecute this action vigorously.

169. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

170. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

171. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

172. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

173. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

174. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

175. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant failed to timely notify the Plaintiff and the class of the Data Breach;
- b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;
- c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

- d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
- e. Whether Defendant failed to take commercially reasonable steps to safeguard customers' PII; and
- f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT I

Negligence

(On Behalf of Plaintiff and the Class)

176. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

177. Defendant requires its customers, including Plaintiff and Class Members, to submit non-public PII in the ordinary course of providing its services.

178. Defendant gathered and stored the PII of Plaintiff and Class Members as part of its business of soliciting its services to its customers, which solicitations and services affect commerce.

179. Plaintiff and Class Members entrusted Defendant with their PII with the understanding that Defendant would safeguard their information.

180. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

181. By voluntarily undertaking and assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty

of care to use reasonable means to secure and safeguard their computer property—and Class Members’ PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant’s duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

182. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

183. Defendant's duty to use reasonable security measures also arose under the GLBA, under which they were required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

184. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks adequately protected the PII.

185. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between CFCU and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted CFCU with their confidential PII, a necessary part of being customers at Defendant.

186. Defendant’s duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

187. Defendant was subject to an “independent duty,” untethered to any contract between Defendant and Plaintiff or the Class.

188. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers’ PII it was no longer required to retain pursuant to regulations.

189. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

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

191. Defendant breached its duties, pursuant to the FTC Act, GLBA, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members’ PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members’ PII;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Allowing unauthorized access to Class Members’ PII;
- d. Failing to detect in a timely manner that Class Members’ PII had been compromised;
- e. Failing to remove former customers’ PII it was no longer required to retain pursuant to regulations, and

- f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

192. Defendant violated Section 5 of the FTC Act and GLBA by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

193. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act and GLBA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm that the statutes were intended to guard against.

194. Defendant's violation of Section 5 of the FTC Act and GLBA constitutes negligence.

195. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

196. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

197. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial services industry.

198. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

199. Plaintiff and the Class 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 the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems or transmitted through third party systems.

200. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

201. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

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

203. 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. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

204. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

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

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

207. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (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) Plaintiff experiencing fraudulent charges to his Chase credit card, totaling approximately \$2,000, in or about May 2024; (viii) Plaintiff's PII being disseminated on the dark web, according to Chase; (ix) actual misuse of their PII consisting of an increase in spam calls, texts, and/or emails; statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their PII, 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 PII.

208. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain 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 PII in its continued possession.

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

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

COUNT II
Breach Of Implied Contract
(On Behalf of Plaintiff and the Class)

211. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

212. Plaintiff and Class Members were required deliver their PII to Defendant as part of the process of obtaining services provided by Defendant. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services.

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

214. Defendant accepted possession of Plaintiff' and Class Members' PII for the purpose of providing services to Plaintiff and Class Members.

215. Plaintiff and the Class entrusted their PII 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.

216. 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 GLBA and FTC guidelines on data security) and were consistent with industry standards.

217. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

218. 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.

219. 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 PII under certain circumstances, none of which relate to the Data Breach.

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

221. Plaintiff and Class Members 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.

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

223. Plaintiff and Class Members would not have entrusted their PII 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.

224. Every contract in this State 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.

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

226. 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.

227. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PII, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of PII 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.

228. 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 PII; (iii) lost or diminished value of PII; (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) Plaintiff experiencing fraudulent charges to his

Chase credit card, totaling approximately \$2,000, in or about May 2024; (viii) Plaintiff's PII being disseminated on the dark web, according to Chase; (ix) actual misuse of their PII consisting of an increase in spam calls, texts, and/or emails; statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their PII, 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 PII.

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

230. 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.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

231. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

232. Plaintiff brings this Count in the alternative to the breach of implied contract count above.

233. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they paid Defendant for services and in so doing also provided Defendant with their PII. In exchange, Plaintiff and Class Members should have received from Defendant the services

that were the subject of the transaction and should have had their PII protected with adequate data security.

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

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

236. Defendant acquired the PII through inequitable means as it failed to investigate and/or disclose the inadequate data security practices previously alleged.

237. If Plaintiff and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would have entrusted their PII at Defendant or obtained services at Defendant.

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

239. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. 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 PII.

240. 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.

241. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (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) Plaintiff experiencing fraudulent charges to his Chase credit card, totaling approximately \$2,000, in or about May 2024; (viii) Plaintiff's PII being disseminated on the dark web, according to Chase; (ix) actual misuse of their PII consisting of an increase in spam calls, texts, and/or emails; statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their PII, 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 PII.

242. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

243. Plaintiff and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT IV
Violation of California’s Unfair Competition Law (“UCL”)
Unlawful Business Practice
(Cal Bus. & Prof. Code § 17200, *et seq.*)
(On Behalf of Plaintiff and the California Subclass)

244. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein, and brings this claim on behalf of himself and the California Subclass (the “Class” for the purposes of this count).

245. Defendant is a “person” defined by Cal. Bus. & Prof. Code § 17201.

246. Defendant violated Cal. Bus. & Prof. Code § 17200 *et seq.* (“UCL”) by engaging in unlawful, unfair, and deceptive business acts and practices.

247. Defendant’s “unfair” acts and practices include:

- a. by utilizing cheaper, ineffective security measures and diverting those funds to its own profit, instead of providing a reasonable level of security that would have prevented the hacking incident;
- b. failing to follow industry standard and the applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data;
- c. failing to timely and adequately notify Class Members about the Data Breach’s occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages;
- d. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff’s and Class Members’ personal information; and

- e. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' personal information.

248. Defendant has engaged in "unlawful" business practices by violating multiple laws, including the FTC Act, 15 U.S.C. § 45, and California common law.

249. Defendant's unlawful, unfair, and deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' personal information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and GLBA, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' personal information, including by implementing and maintaining reasonable security measures; and
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and GLBA.

250. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' personal information.

251. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiff and Class Members' were injured and lost money or property, which would not have occurred but for the unfair and deceptive acts, practices, and omissions alleged herein, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personal information.

252. Defendant's violations were, and are, willful, deceptive, unfair, and unconscionable.

253. Plaintiff and Class Members have lost money and property as a result of Defendant's conduct in violation of the UCL, as stated herein and above.

254. By deceptively storing, collecting, and disclosing their personal information, Defendant has taken money or property from Plaintiff and Class Members.

255. Defendant acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and Class Members' rights.

256. Plaintiff and Class Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent business practices or use of their personal information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

COUNT V
Violation of the California Consumer Privacy Act of 2018 ("CCPA")
Cal. Civ. Code § 1798, *et seq.*
(On Behalf of Plaintiff and the California Subclass)

257. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein, and brings this claim on behalf of himself and the California Subclass (the "Class" for the purposes of this count).

258. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides:

Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

(A) To recover damages in an amount not less than one hundred dollars (\$100) and not greater than seven hundred and fifty (\$750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

259. Defendant is a "business" under § 1798.140(b) in that it is a corporation organized for profit or financial benefit of its shareholders or other owners, with gross revenue in excess of \$25 million.

260. Plaintiff and Class Members are covered "consumers" under § 1798.140(g) in that they are natural persons who are California residents.

261. The personal information of Plaintiff and the Class Members at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and 1798.81.5, in that the personal

information Defendant collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

262. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Class Members' personal information and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the Class Members. Specifically, Defendant subjected Plaintiff's and the Class Members' nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

263. As a direct and proximate result of Defendant's violation of its duty, the unauthorized access and exfiltration, theft, or disclosure of Plaintiff's and Class Members' personal information included exfiltration, theft, or disclosure through Defendant's servers,

systems, and website, and/or the dark web, where hackers further disclosed the personal identifying information alleged herein.

264. As a direct and proximate result of Defendant's acts, Plaintiff and the Class Members were injured and lost money or property, including but not limited to the loss of Plaintiff's and Class Members' legally protected interest in the confidentiality and privacy of their personal information, stress, fear, and anxiety, nominal damages, and additional losses described above.

265. Section 1798.150(b) specifically provides that "[n]o [prefiling] notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages."

266. On May 31, 2024, Plaintiff's counsel sent a CCPA notice letter to Defendant's registered service agents via certified mail. If Defendant does not cure the effects of the Data Breach, which would require retrieving the PII and securing the PII from continuing and future use, within 30 days of delivery of such CCPA notice letter (which Plaintiff believes any such cure is not possible under these facts and circumstances), Plaintiff shall seek actual damages and statutory damages of no less than \$100 and up to \$750 per customer record subject to the Data Breach on behalf of the California Subclass as authorized by the CCPA.

267. Accordingly, Plaintiff and the Class Members by way of this complaint seek actual pecuniary damages suffered as a result of Defendant's violations described herein.

COUNT VI
Violation of the California Customer Records Act,
Cal. Civ. Code § 1798.80 *et seq.*
(On Behalf of Plaintiff and the California Subclass)

268. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein, and brings this claim on behalf of himself and the California Subclass (the "Class" for the purposes of this count).

269. Cal. Civ. Code § 1798.81.5 provides that “[i]t is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information.”

270. Section 1798.81.5(b) further states that: “[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.”

271. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a violation of this title may institute a civil action to recover damages.” Section 1798.84(e) further provides that “[a]ny business that violates, proposes to violate, or has violated this title may be enjoined.”

272. Plaintiff and the Class Members are “customers” within the meaning of Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals who provided personal information to Defendant for the purpose of obtaining services from Defendant.

273. The personal information of Plaintiff and the Class Members at issue in this lawsuit constitutes “personal information” under § 1798.81.5(d)(1) in that the personal information Defendant collects and which was impacted by the cybersecurity attack includes an individual’s first name or first initial and the individual’s last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) Driver’s license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any

required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

274. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Plaintiff's and Class Members' personal information and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the Class Members. Specifically, Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information of Plaintiff and the Class Members from unauthorized access, destruction, use, modification, or disclosure. Defendant further subjected Plaintiff's and the Class Members' nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

275. As a direct and proximate result of Defendant's violation of its duty, the unauthorized access, destruction, use, modification, or disclosure of the personal information of Plaintiff and the Class Members included hackers' access to, removal, deletion, destruction, use, modification, disabling, disclosure and/or conversion of the personal information of Plaintiff and the Class Members by the cyber attackers and/or additional unauthorized third parties to whom those cybercriminals sold and/or otherwise transmitted the information.

276. As a direct and proximate result of Defendant's acts or omissions, Plaintiff and the Class Members were injured and lost money or property including, but not limited to, the loss of Plaintiff's and the Class Members' legally protected interest in the confidentiality and privacy of their personal information, nominal damages, and additional losses described above. Plaintiff seeks compensatory damages as well as injunctive relief pursuant to Cal. Civ. Code § 1798.84(b).

277. Moreover, the California Customer Records Act further provides: "A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82.

278. Any person or business that is required to issue a security breach notification under the CRA must meet the following requirements under §1798.82(d):

- a. The name and contact information of the reporting person or business subject to this section;
- b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;
- c. If the information is possible to determine at the time the notice is provided, then any of the following:
 - i. the date of the breach,
 - ii. the estimated date of the breach, or
 - iii. the date range within which the breach occurred.

- d. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;
- e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided;
- f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number;
- g. If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information.

279. Defendant failed to provide the legally compliant notice under § 1798.82(d) to Plaintiff and members of the Class. On information and belief, to date, Defendant has not sent written notice of the data breach to all impacted individuals. As a result, Defendant has violated § 1798.82 by not providing legally compliant and timely notice to all Class Members. Because not all members of the class have been notified of the breach, members could have taken action to protect their personal information, but were unable to do so because they were not timely notified of the breach.

280. On information and belief, many Class Members affected by the breach have not received any notice at all from Defendant in violation of Section 1798.82(d).

281. As a result of the violations of Cal. Civ. Code § 1798.82, Plaintiff and Class Members suffered incrementally increased damages separate and distinct from those simply caused by the breaches themselves.

282. As a direct consequence of the actions as identified above, Plaintiff and Class Members incurred additional losses and suffered further harm to their privacy, including but not limited to economic loss, the loss of control over the use of their identity, increased stress, fear, and anxiety, harm to their constitutional right to privacy, lost time dedicated to the investigation of the breach and effort to cure any resulting harm, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal, financial, and payroll information disclosed, that they would not have otherwise incurred, and are entitled to recover compensatory damages according to proof pursuant to § 1798.84(b).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grants the following:

- A. For an Order certifying the Classes, and appointing Plaintiff and his Counsel to represent the Classes;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members;

- C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
- i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
 - iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
 - iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff's and Class Members' respective lifetimes;
 - v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;
 - vi. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;
 - vii. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct

- testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- viii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
 - ix. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
 - x. requiring Defendant to segment data by, among other things, creating firewalls and controls so that if one area of Defendant's network is compromised, hackers cannot gain access to portions of Defendant's systems;
 - xi. requiring Defendant to conduct regular database scanning and securing checks;
 - xii. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
 - xiii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
 - xiv. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding

- subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
- xv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
 - xvi. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect himself;
 - xvii. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and
 - xviii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;
- D. For an award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;
 - E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
 - F. For prejudgment interest on all amounts awarded; and

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

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all claims so triable.

Dated: May 31, 2024

Respectfully Submitted,

By: /s/ David K. Lietz

David K. Lietz

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, PLLC

5335 Wisconsin Avenue NW, Suite 440

Washington, D.C. 20015-2052

Telephone: (866) 252-0878

Facsimile: (202) 686-2877

dlietz@milberg.com

Gary M. Klinger

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, PLLC

227 W. Monroe Street, Suite 2100

Chicago, IL 60606

Phone: (866) 252-0878

gklinger@milberg.com

Counsel for Plaintiff and the Proposed Class

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

Place an "X" in the appropriate box (required): Green Bay Division Milwaukee Division

I. (a) PLAINTIFFS

MATTHEW THOMSON, on behalf of himself and all others similarly situated

(b) County of Residence of First Listed Plaintiff Marin County, CA
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

David K. Lietz, Milberg Coleman Bryson Phillips Grossman, PLLC,
5335 Wisconsin Ave. NW, Suite 440, Washington, D.C. 20015; (866) 252-0878

DEFENDANTS

COMMUNITY FIRST CREDIT UNION

County of Residence of First Listed Defendant Outagamie County, WI
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)
Not Known

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- 1 U.S. Government Plaintiff
- 2 U.S. Government Defendant
- 3 Federal Question (U.S. Government Not a Party)
- 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- | | | | | | |
|---|---------------------------------------|----------------------------|---|----------------------------|---------------------------------------|
| | PTF | DEF | | PTF | DEF |
| Citizen of This State | <input type="checkbox"/> 1 | <input type="checkbox"/> 1 | Incorporated or Principal Place of Business In This State | <input type="checkbox"/> 4 | <input checked="" type="checkbox"/> 4 |
| Citizen of Another State | <input checked="" type="checkbox"/> 2 | <input type="checkbox"/> 2 | Incorporated and Principal Place of Business In Another State | <input type="checkbox"/> 5 | <input type="checkbox"/> 5 |
| Citizen or Subject of a Foreign Country | <input type="checkbox"/> 3 | <input type="checkbox"/> 3 | Foreign Nation | <input type="checkbox"/> 6 | <input type="checkbox"/> 6 |

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Click here for: [Nature of Suit Code Descriptions.](#)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
<input type="checkbox"/> 110 Insurance	PERSONAL INJURY	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881	<input type="checkbox"/> 422 Appeal 28 USC 158	<input type="checkbox"/> 375 False Claims Act
<input type="checkbox"/> 120 Marine	<input type="checkbox"/> 310 Airplane	<input type="checkbox"/> 690 Other	<input type="checkbox"/> 423 Withdrawal 28 USC 157	<input type="checkbox"/> 376 Qui Tam (31 USC 3729(a))
<input type="checkbox"/> 130 Miller Act	<input type="checkbox"/> 315 Airplane Product Liability		PROPERTY RIGHTS	<input type="checkbox"/> 400 State Reapportionment
<input type="checkbox"/> 140 Negotiable Instrument	<input type="checkbox"/> 320 Assault, Libel & Slander		<input type="checkbox"/> 820 Copyrights	<input type="checkbox"/> 410 Antitrust
<input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment	<input type="checkbox"/> 330 Federal Employers' Liability		<input type="checkbox"/> 830 Patent	<input type="checkbox"/> 430 Banks and Banking
<input type="checkbox"/> 151 Medicare Act	<input type="checkbox"/> 340 Marine		<input type="checkbox"/> 835 Patent - Abbreviated New Drug Application	<input type="checkbox"/> 450 Commerce
<input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans)	<input type="checkbox"/> 345 Marine Product Liability		<input type="checkbox"/> 840 Trademark	<input type="checkbox"/> 460 Deportation
<input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits	<input type="checkbox"/> 350 Motor Vehicle	LABOR	<input type="checkbox"/> 880 Defend Trade Secrets Act of 2016	<input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations
<input type="checkbox"/> 160 Stockholders' Suits	<input type="checkbox"/> 355 Motor Vehicle Product Liability	<input type="checkbox"/> 710 Fair Labor Standards Act		<input type="checkbox"/> 480 Consumer Credit (15 USC 1681 or 1692)
<input type="checkbox"/> 190 Other Contract	<input checked="" type="checkbox"/> 360 Other Personal Injury	<input type="checkbox"/> 720 Labor/Management Relations	SOCIAL SECURITY	<input type="checkbox"/> 485 Telephone Consumer Protection Act
<input type="checkbox"/> 195 Contract Product Liability	<input type="checkbox"/> 362 Personal Injury - Medical Malpractice	<input type="checkbox"/> 740 Railway Labor Act	<input type="checkbox"/> 861 HIA (1395ff)	<input type="checkbox"/> 490 Cable/Sat TV
<input type="checkbox"/> 196 Franchise		<input type="checkbox"/> 751 Family and Medical Leave Act	<input type="checkbox"/> 862 Black Lung (923)	<input type="checkbox"/> 850 Securities/Commodities/Exchange
		<input type="checkbox"/> 790 Other Labor Litigation	<input type="checkbox"/> 863 DIWC/DIWW (405(g))	<input type="checkbox"/> 890 Other Statutory Actions
REAL PROPERTY	CIVIL RIGHTS	<input type="checkbox"/> 791 Employee Retirement Income Security Act	<input type="checkbox"/> 864 SSID Title XVI	<input type="checkbox"/> 891 Agricultural Acts
<input type="checkbox"/> 210 Land Condemnation	<input type="checkbox"/> 440 Other Civil Rights		<input type="checkbox"/> 865 RSI (405(g))	<input type="checkbox"/> 893 Environmental Matters
<input type="checkbox"/> 220 Foreclosure	<input type="checkbox"/> 441 Voting	IMMIGRATION	FEDERAL TAX SUITS	<input type="checkbox"/> 895 Freedom of Information Act
<input type="checkbox"/> 230 Rent Lease & Ejectment	<input type="checkbox"/> 442 Employment Accommodations	<input type="checkbox"/> 462 Naturalization Application	<input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant)	<input type="checkbox"/> 896 Arbitration
<input type="checkbox"/> 240 Torts to Land	<input type="checkbox"/> 445 Amer. w/Disabilities - Employment	<input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 871 IRS—Third Party 26 USC 7609	<input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision
<input type="checkbox"/> 245 Tort Product Liability	<input type="checkbox"/> 446 Amer. w/Disabilities - Other			<input type="checkbox"/> 950 Constitutionality of State Statutes
<input type="checkbox"/> 290 All Other Real Property	<input type="checkbox"/> 448 Education			
	PRISONER PETITIONS			
	Habeas Corpus:			
	<input type="checkbox"/> 463 Alien Detainee			
	<input type="checkbox"/> 510 Motions to Vacate Sentence			
	<input type="checkbox"/> 530 General			
	<input type="checkbox"/> 535 Death Penalty			
	Other:			
	<input type="checkbox"/> 540 Mandamus & Other			
	<input type="checkbox"/> 550 Civil Rights			
	<input type="checkbox"/> 555 Prison Condition			
	<input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN (Place an "X" in One Box Only)

- 1 Original Proceeding
- 2 Removed from State Court
- 3 Remanded from Appellate Court
- 4 Reinstated or Reopened
- 5 Transferred from Another District (specify)
- 6 Multidistrict Litigation - Transfer
- 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):

28 U.S.C. § 1332(d) and 18 U.S.C. § 1391(b)(1)

Brief description of cause:
Data Breach

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND \$ 5,000,000.00

CHECK YES only if demanded in complaint:

JURY DEMAND: Yes No

VIII. RELATED CASE(S) IF ANY

(See updated instructions):
JUDGE _____

DOCKET NUMBER _____

DATE
05/31/2024

SIGNATURE OF ATTORNEY OF RECORD
/s/ David K. Lietz

FOR OFFICE USE ONLY

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I.(a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
- (b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)
- (c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".
- II. Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
 United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
 United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
 Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
 Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: [Nature of Suit Code Descriptions](#).
- V. Origin.** Place an "X" in one of the seven boxes.
 Original Proceedings. (1) Cases which originate in the United States district courts.
 Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
 Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
 Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
 Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
 Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
 Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket. **PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7.** Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.
- VII. Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
 Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
 Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS 44 is used to reference related pending and **previously filed** cases, if any. If there are related cases, insert the docket numbers and the corresponding judge names for such cases **and file a Notice of Related Action pursuant to Civil L.R. 3(b).**
- Date and Attorney Signature.** Date and sign the civil cover sheet.

UNITED STATES DISTRICT COURT
for the
Eastern District of Wisconsin

MATTHEW THOMSON, on behalf of himself and all oth

Plaintiff(s)

v.

COMMUNITY FIRST CREDIT UNION

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: (Defendant's name and address) COMMUNITY FIRST CREDIT UNION
c/o Registered Agent
1575 Dresang Way
Neenah, WI

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you receive it) – or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12(a)(2) or (3) – you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or the plaintiff's attorney, whose name and address are:

David K. Lietz
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW, Suite 440
Washington, D.C. 20015

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

GINA M. COLLETTI, CLERK OF COURT

Date:

Signature of Clerk or Deputy Clerk

Civil Action No. _____

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4(l))

This summons and the attached complaint for *(name of individual and title, if any)*:

were received by me on *(date)* _____.

I personally served the summons and the attached complaint on the individual at *(place)*:

_____ on *(date)* _____ ; or

I left the summons and the attached complaint at the individual's residence or usual place of abode with *(name)*

_____, a person of suitable age and discretion who resides there,

on *(date)* _____, and mailed a copy to the individual's last known address; or

I served the summons and the attached complaint on *(name of individual)* _____

who is designated by law to accept service of process on behalf of *(name of organization)* _____

_____ on *(date)* _____ ; or

I returned the summons unexecuted because _____ ; or

Other *(specify)*: _____

My fees are \$ _____ for travel and \$ _____ for services, for a total of \$ _____ 0.00

I declare under penalty of perjury that this information is true.

Date: _____

Server's signature

Printed name and title

Server's address

Additional information regarding attempted service, etc.: