IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

JOSHUA AMBROSE-MANNESS, individually and on behalf of all others similarly situated, ***Plaintiff,*** **v.** **FIRST COMMONWEALTH FEDERAL CREDIT UNION,** ***Defendant.***	**Case No.:** 5:24-cv-4358 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff, Joshua Ambrose-Manness, ("Plaintiff") brings this Class Action Complaint against Defendant, First Commonwealth Federal Credit Union ("Defendant") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to Plaintiff's own actions and to counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard the personally identifiable information ("PII") of its customers, including, but not limited to: full names, Social Security numbers, addresses, dates of birth, and account numbers.

2. Defendant is an institution that is significantly engaged in financial activities, or significantly engaged in activities incidental to such financial activities, such as issuing: checking accounts, savings accounts, home equity lines of credit, and credit cards. Defendant requires customers to provide their PII in connection with the transaction.

3. Defendant's website states, in part, "**Your Privacy, Our Priority**. Service excellence is important to us, especially when it comes to protecting your privacy. Our Privacy Policy is designed to protect the financial relationship that we have with you. The credit union collects nonpublic personal information about you when you submit applications and forms for savings and/or lending services. Other sources of nonpublic personal information are your account transaction activity, credit history on file with consumer reporting agencies and information from marketing research firms. *First Commonwealth Federal Credit Union does not disclose nonpublic information to affiliated or non-affiliated third parties except as allowed by law*. The law allows us to exchange account activity information with third parties in order to process things such as ATM and check card activity and open credit line activity. *Our staff is committed to protecting your personal information*."[1]

4. Defendant's published privacy policy further provides, "[t]o protect your personal information from unauthorized access and use, we use security

[1] https://www.firstcomcu.org/privacypolicy.html

measures that comply with federal law. These measures include computer safeguards and secured files and buildings."[2]

5. On, or about, June 27, 2024, Defendant detected unusual activity in its information technology systems and determined that Plaintiff's personal information—which was entrusted to Defendant on the mutual understanding that Defendant would protect it against unauthorized disclosure—was accessed and exfiltrated in a data breach (hereafter referred to as the "Data Breach").

6. On, or about, August 2, 2024, Defendant sent out data breach notice letters to the Plaintiff and other individuals who were affected by the data breach. In the letter, Defendant stated that, as a result of the Data Breach, it "further strengthened [its] existing security policies and procedures" and "bolstered security to further protect against similar incidents in the future."

7. Omitted from the data breach notice letter were 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, who retains a vested interest in ensuring that his PII remains protected.

8. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's PII was a known risk to Defendant,

[2] https://www.firstcomcu.org/content/docs/Privacy-Policy-7-15-19-PC.pdf

and thus, Defendant was on notice that failing to take steps necessary to secure the PII from those risks left the data in a dangerous condition.

9. The Data Breach was a direct result of Defendant's failure to implement an information security program designed to: (a) to ensure the security and confidentiality of customer information; (b) to protect against anticipated threats or hazards to the security or integrity of that information; and (c) to protect against unauthorized access to that information that could result in substantial harm or inconvenience to any customer.

10. An information security program encompasses the administrative, technical, or physical safeguards used to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information. Had Defendant implemented an information security program consistent with industry standards and best practices, it could have prevented the Data Breach.

11. As a result of the Data Breach, Plaintiff has suffered an actual injury, similar to an intangible harm remedied at common law. Defendant's failure to implement an information security program resulted in the unauthorized disclosure of Plaintiff's private information to cybercriminals. The unauthorized disclosure of Plaintiff's PII constitutes an invasion of a legally protected privacy interest, that is traceable to the Defendant's failure to adequately secure the PII in its custody, and has resulted in actual, particularized, and concrete harm to the Plaintiff. The injuries

Plaintiff suffered, as described herein, can be redressed by a favorable decision in this matter.

12. Defendant has not provided any assurances that: all data acquired in the Data Breach, or copies thereof, have been recovered or destroyed; or, that Defendant has modified its data protection policies, procedures, and practices sufficient to avoid future, similar, data breaches.

13. Defendant's conduct, as evidenced by the circumstances of the Data Breach, has created a substantial risk of future identity theft, fraud, or other forms of exploitation. The circumstances demonstrating a substantial risk of future exploitation include, but are not limited to:

a. **Sensitive Data Type**: The data acquired in the Data Breach included unencrypted Social Security numbers, addresses, dates of birth, and account numbers. Upon information and belief, this category of data is used by cybercriminals to perpetuate fraud, identity theft, and other forms of exploitation.[3]

b. **Data Misuse**: On, or about, August 12, 2024, Plaintiff discovered the data acquired in the Data Breach might have been leaked on the dark web. The dark web uses a series of encrypted networks to hide users' identities, which makes it convenient for criminals to buy and sell illegally obtained data. Many criminals purchase stolen personal data off the dark web before launching social engineering-based attacks. A social engineering attack is a method of using psychological manipulation to deceive a victim and gain access to a computer system or to steal sensitive information such as login credentials. Social engineering attacks that can be launched using names, telephone numbers and email addresses include phishing, smishing (SMS message), vishing (voice messaging), pretexting, and baiting attacks.

[3] https://www.f-secure.com/us-en/articles/why-do-hackers-want-your-personal-information

14. The imminent risk of future harm resulting from the Data Breach is traceable to the Defendant's failure to adequately secure the PII in its custody, and has created a separate, particularized, and concrete harm to the Plaintiff.

15. More specifically, the Plaintiff's exposure to the substantial risk of future exploitation caused them to: (i) spend time and money on mitigation measures like credit monitoring services and/or dark web searches; (ii) lose time and effort spent responding to the Data Breach; and/or (iii) experience emotional distress associated with reviewing accounts for fraud, changing usernames and passwords or closing accounts to prevent fraud, and general anxiety over the consequences of the Data Breach. The harm Plaintiff suffered can be redressed by a favorable decision in this matter.

16. Armed with the PII acquired in the Data Breach, data thieves have already engaged in theft and can, in the future, commit a variety of crimes including, opening new financial accounts, taking out loans, using Plaintiff's information to obtain government benefits, file fraudulent tax returns, obtain driver's licenses, and give false information to police during an arrest.

17. As a result of the Data Breach, Plaintiff suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of 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) an

increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and increased risk their PII will be further misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access on the dark web or otherwise; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the data.

18. Plaintiff brings this class action lawsuit individually, and on behalf of all those similarly situated, to address Defendant's inadequate data protection practices and for failing to provide timely and adequate notice of the Data Breach.

19. Through this Complaint, Plaintiff seeks to remedy these harms individually, and on behalf of all similarly situated individuals whose PII was accessed during the Data Breach. Plaintiff has a continuing interest in ensuring that personal information is kept confidential and protected from disclosure, and Plaintiff should be entitled to injunctive and other equitable relief.

JURISDICTION & VENUE

20. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C.§1332, because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000.00, exclusive of interest and costs, there are more than 100 members in

the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

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

22. Venue is proper under 28 U.S.C §1391(b) because Defendant maintains a principal place of business in this District and a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

PARTIES

23. Plaintiff Joshua Ambrose-Manness is a citizen of the Commonwealth of Pennsylvania. At all relevant times, Plaintiff has been a resident of Nesquehoning, Carbon County, Pennsylvania.

24. Defendant, First Commonwealth Federal Credit Union, maintains a principal place of business at 6126 Hamilton Boulevard, Suite 100, Allentown, Lehigh County, Pennsylvania 18106.

FACTUAL ALLEGATIONS

25. Defendant is a member-owned, not-for-profit cooperative financial institution serving over 94,000 members and requires customers to provide their PII in connection with each financial transaction.

26. Plaintiff and Class Members (later defined) are current and former customers of Defendant's various services.

27. In the course of their relationship, Plaintiff and Class Members, provided Defendant with at least the following: full names, dates of birth, and Social Security numbers.

28. Defendant promised to use reasonable technical, administrative, and physical safeguards to protect the PII it collected. These promises were contained in the applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

29. Plaintiff and the Class Members, as customers of Defendant, relied on these representations and on this sophisticated business entity to keep their PII confidential, securely maintained, and to make only authorized disclosures of this information.

30. On, or about, June 27, 2024, Defendant detected unusual activity in its information technology systems and determined that Plaintiff's personal information was accessed and exfiltrated in the Data Breach.

31. On or about August 2, 2024, Defendant sent a data breach notice letter to Plaintiff and other individuals who were affected by the data breach.

Data Breaches Are Avoidable

32. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's 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 the data in a dangerous condition.

33. Upon information and belief, the Data Breach was a direct result of Defendant's failure to: (i) identify risks and potential effects of collecting, maintaining, and sharing personal information; (ii) adhere to its published privacy practices; (iii) implement reasonable data protection measures for the collection, use, disclosure, and storage of personal information; and/or (iv) ensure its third-party vendors were required to implement reasonable data protection measures consistent with Defendant's data protection obligations.

34. Upon information and belief, the Defendant was impacted by a ransomware attack. In a ransomware attack, the attackers use software to encrypt data on a compromised network, rendering it unusable and then demand payment to restore control over the network.[4] Ransomware groups frequently implement a double extortion tactic, "where the cybercriminal **posts portions of the data** to increase their leverage and force the victim to pay the ransom, and then sells the

[4] *Ransomware FAQs*, https://www.cisa.gov/stopransomware/ransomware-faqs (accessed June 11, 2024).

stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[5]

35. Upon information and belief, the Data Breach occurred as a result of a phishing attack. A phishing attack involves the use of fraudulent emails, social media messages, text messages, websites, or other communication to obtain login credentials or other sensitive information. Phishing attacks are prevalent because they exploit human vulnerabilities. Cybercriminals can use phishing attacks to "trick people who have authorized access to their target—be it money, sensitive information or something else—into doing their dirty work."[6]

36. To detect and prevent cyber-attacks, Defendant could and should have implemented the following measures:

Reasonable Safeguards

a. Regularly patch critical vulnerabilities in operating systems, software, and firmware on devices. Consider using a centralized patch management system.
b. Check expert websites (such as www.us-cert.gov) and your software vendors' websites regularly for alerts about new vulnerabilities and implement policies for installing vendor-approved patches to correct problems.
c. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks. Depending on your circumstances, appropriate assessments may range from having a knowledgeable

[5] *Ransomware: The Data Exfiltration and Double Extortion Trends*, https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends (accessed June 11, 2024).
[6] *What is phishing?* IBM security topics, https://www.ibm.com/topics/phishing (accessed June 11, 2024).

employee run off-the-shelf security software to having an independent professional conduct a full-scale security audit.

d. Scan computers on your network to identify and profile the operating system and open network services. If you find services that you don't need, disable them to prevent hacks or other potential security problems.

e. 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.

f. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email.

g. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

h. Configure firewalls to block access to known malicious IP addresses.

i. Set anti-virus and anti-malware programs to conduct regular scans automatically.

j. 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.

k. 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.

l. 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.

m. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

n. Consider disabling Remote Desktop protocol (RDP) if it is not being used.

o. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

p. Execute operating system environments or specific programs in a virtualized environment.

q. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

r. Conduct an annual penetration test and vulnerability assessment.

s. Secure your backups.[7]

t. Identify the computers or servers where sensitive personal information is stored.

u. Identify all connections to the computers where you store sensitive information. These may include the internet, electronic cash registers, computers at your branch offices, computers used by service providers to support your network, digital copiers, and wireless devices like smartphones, tablets, or inventory scanners.

v. Don't store sensitive consumer data on any computer with an internet connection unless it's essential for conducting your business.

w. Encrypt sensitive information that you send to third parties over public networks (like the internet) and encrypt sensitive information that is stored on your computer network, laptops, or portable storage devices used by your employees. Consider also encrypting email transmissions within your business.

x. Regularly run up-to-date anti-malware programs on individual computers and on servers on your network.

y. Restrict employees' ability to download unauthorized software. Software downloaded to devices that connect to your network (computers, smartphones, and tablets) could be used to distribute malware.

z. To detect network breaches when they occur, consider using an intrusion detection system.

[7] *How to Protect Your Networks from Ransomware*, at p.3, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (accessed June 11, 2024).

aa. Create a "culture of security" by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities.

bb. Tell employees about your company policies regarding keeping information secure and confidential. Post reminders in areas where sensitive information is used or stored, as well as where employees congregate.

cc. Teach employees about the dangers of spear phishing—emails containing information that makes the emails look legitimate. These emails may appear to come from someone within your company, generally someone in a position of authority. Make it office policy to independently verify any emails requesting sensitive information.

dd. Before you outsource any of your business functions investigate the company's data security practices and compare their standards to yours.[8]

37. The Federal Trade Commission's Standards for Safeguarding Customer Information (the "Safeguards Rule") 16 CFR §314, requires financial institutions to develop, implement, and maintain an information security program with administrative, technical, and physical safeguards designed to protect customer information. The primary requirements of an information security program are:

a. Designate a qualified individual to implement and supervise the information security program.

b. Conduct an assessment to determine foreseeable risks and threats – internal and external – to the security, confidentiality, and integrity of customer information.

c. Design and implement safeguards to control the risks identified through the risk assessment.

[8] *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (accessed June 11, 2024).

d. Regularly monitor and test the effectiveness of the chosen safeguards.

e. Provide staff with security awareness training and schedule regular refreshers.

f. Select service providers with the skills and experience to maintain appropriate safeguards. Include security expectations in vendor contracts, monitor the service provider's work, and provide for periodic reassessments of their suitability.

g. Ensure the information security program remains current. It should reflect changes to operations, changes based on information gained from risk assessments, changes due to emerging threats, changes in personnel, and changes necessitated by other circumstances that may have a material impact on the information security program.

h. Create a written incident response plan.

i. Require the "Qualified Individual" to report to the Board of Directors, in writing, at least annually.[9]

38. Given that Defendant is a financial institution that collected, used, and stored PII, Defendant could and should have identified the risks and potential effects of collecting, maintaining, and sharing personal information.

39. Without identifying the potential risks to the personal data in Defendant's possession, Defendant could not identify and implement the necessary measures to detect and prevent cyberattacks. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of Plaintiff's and the Class Members' PII.

[9] See, https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know (last accessed August 7, 2024).

40. Defendant knew and understood unencrypted PII is valuable and highly sought after by cybercriminals seeking to illegally monetize that data. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if a data breach occurred, including the significant cost that would be imposed on Plaintiff and the Class Members as a result.

Plaintiff and Class Members Sustained Damages in the Data Breach

41. The invasion of the Plaintiff's and Class Members' privacy suffered in this Data Breach constitutes an actual, particularized, redressable injury traceable to the Defendant's conduct. As a consequence of the Data Breach, Plaintiff and Class Members sustained monetary damages that exceed the sum or value of $5,000,000.00.

42. Additionally, Plaintiff and Class Members face a substantial risk of future identity theft, fraud, or other exploitation where their names, Social Security numbers, dates of birth and financial account numbers were targeted by a sophisticated hacker that typically resells sensitive data on the dark web. The substantial risk of future identity theft and fraud created by the Data Breach constitutes a redressable injury traceable to the Defendant's conduct.

43. Furthermore, Plaintiff and Class Members face a substantial risk of future spam, phishing, or other attacks designed to trick them into sharing sensitive

data, downloading malware, or otherwise exposing themselves to cybercrime, where their names and contact information were acquired in the Data Breach and subsequently released on the dark web. The substantial risk of future exploitation created by the Data Breach constitutes a redressable injury traceable to the Defendant's conduct.

44. Upon information and belief, a criminal can easily link data acquired in the Data Breach with information available from other sources to commit a variety of fraud related crimes. An example of criminals piecing together bits and pieces of data is the development of "Fullz" packages.[10] With "Fullz" packages, cyber-criminals can combine multiple sources of PII to apply for credit cards, loans, assume identities, or take over accounts.

45. Given the type of targeted attack in this case, the sophistication of the criminal responsible for the Data Breach, the type of PII involved in the Data Breach, hackers typical behavior in other similar data breaches, the ability of criminals to link data acquired in the Data Breach with information available from other sources, and the fact that the stolen information has been placed, or will be placed, on the dark web, it is reasonable for Plaintiff and the Class Members to assume that their

[10] "Fullz" is term used by cybercriminals to describe "a package of all the personal and financial records that thieves would need to fraudulently open up new lines of credit in a person's name." A Fullz package typically includes the victim's name, address, credit card information, social security number, date of birth, bank name, routing number, bank account numbers and more. *See, e.g.*, Brian 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-firm

PII was obtained by, or released to, criminals intending to utilize the PII for future identity theft-related crimes or exploitation attempts.

46. The substantial risk of future identity theft, fraud, or other exploitation that Plaintiff and Class Members face is sufficiently concrete, particularized, and imminent that it necessitates the present expenditure of funds to mitigate the risk. Consequently, Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to understand and mitigate the effects of the Data Breach.

47. For example, the Federal Trade Commission has recommended steps that data breach victims take to protect themselves and their children after a data breach, including: (i) 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); (ii) regularly obtaining and reviewing their credit reports; (iii) removing fraudulent charges from their accounts; (iv) closing new accounts opened in their name; (v) placing a credit freeze on their credit; (vi) replacing government-issued identification; (vii) reporting misused Social Security numbers; (viii) contacting utilities to ensure no one obtained cable, electric, water, or other similar services in their name; and (ix) correcting their credit reports.[11]

[11]*See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps

48. As a consequence of the Data Breach, Plaintiff and Class Members sustained or will incur monetary damages to mitigate the effects of an imminent risk of future injury. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year. The cost of dark web scanning and monitoring services can cost around $180 per year.

49. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and illegitimate markets, has been damaged and diminished by its 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.

50. Personal information is of great value; in 2019, the data brokering industry was worth roughly $200 billion.[12] Data such as name, address, phone number, and credit history has been sold at prices ranging from $40 to $200 per record.[13] Sensitive PII can sell for as much as $363 per record.[14]

[12] *Column: Shadowy data brokers make the most of their invisibility cloak*, https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[13] *In the Dark*, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/

[14] *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).

51. Furthermore, Defendant's poor data security practices deprived Plaintiff and Class Members of the benefit of their bargain. By transacting business with Plaintiff and Class Members, collecting their PII, using their PII for profit or to improve the ability to make profits, and then permitting the unauthorized disclosure of the PII, Plaintiff and Class Members were deprived of the benefit of their bargain.

52. When agreeing to pay Defendant for products or services, consumers understood and expected that they were, in part, paying for the protection of their personal data, when in fact, Defendant did not invest the funds into implementing reasonable data security practices. 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.

53. Through this Complaint, Plaintiff seeks redress individually, and on behalf of all similarly situated individuals, for the damages that resulted from the Data Breach.

CLASS ALLEGATIONS

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

55. The Class that Plaintiff seeks to represent is defined as follows:

Nationwide Class

All individuals residing in the United States whose PII was accessed and acquired by an unauthorized party as a result of a data breach that was discovered on, or about, June 27, 2024, as reported by Defendant First Commonwealth Federal Credit Union, (the "Class").

Pennsylvania Subclass

All individuals residing in the Commonwealth of Pennsylvania whose PII was accessed and acquired by an unauthorized party as a result of a data breach that was discovered on, or about, June 27, 2024, as reported by Defendant First Commonwealth Federal Credit Union, (the "Pennsylvania Subclass").

56. Collectively, the Class and Pennsylvania Subclass are referred to as the "Classes" or "Class Members."

57. 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 has 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.

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

59. Numerosity: The members of the Classes are so numerous that joinder of all members is impracticable, if not completely impossible. The members of the Classes are so numerous that joinder of all of them is impracticable. While the exact

number of Class Members is unknown to Plaintiff at this time and such number is exclusively in the possession of Defendant, upon information and belief 98,809 individuals were impacted in Data Breach.

60. Common questions of law and fact exist as to all members of the Classes and predominate over any questions affecting solely individual members of the Classes. The questions of law and fact common to the Classes that predominate over questions which may affect individual Class Members, includes 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 a duty not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;
c. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;
d. Whether Defendant required its third-party vendors to adequately safeguard the PII of Plaintiff and Class Members;
e. 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 practices, procedures, or 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 ongoing harm faced as a result of the Data Breach.

61. Typicality: Plaintiff's claims are typical of those of the other members of the Classes 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 Classes.

62. 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 Classes, 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 Classes 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 Classes as a whole, not on facts or law applicable only to Plaintiff.

63. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff 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 suffered are typical of other Class Members. Plaintiff has

retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

64. 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.

65. 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 for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since Defendant 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 Classes 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.

66. 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 demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

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

68. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Classes, 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.

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

70. 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 Classes of the Data Breach;
b. Whether Defendant owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, sharing, storing, and safeguarding their PII;
c. Whether Defendant's (or their vendors') security measures to protect its network were reasonable in light of industry best practices;
d. Whether Defendant's (or their vendors') failure to institute adequate data protection measures amounted to negligence;
e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII;
f. Whether Defendant made false representations about their data privacy practices and commitment to the security and confidentiality of customer information; and
g. Whether adherence to FTC recommendations and best practices for protecting personal information would have reasonably prevented the Data Breach.

CAUSES OF ACTION
(*On behalf of Plaintiff and the Classes*)

COUNT 1: NEGLIGENCE/NEGLIGENCE *PER SE*

71. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

72. Defendant requires their customers, including Plaintiff and Class Members, to submit PII in the ordinary course of providing products or services.

73. Defendant gathered and stored the PII of Plaintiff and Class Members as part of its business of soliciting its services to customers. Plaintiff and Class Members entrusted Defendant with their PII with the understanding that Defendant would adequately safeguard their information.

74. Defendant had full knowledge of the types of PII it collected and the types of harm that Plaintiff and Class Members would suffer if that data was accessed and exfiltrated by an unauthorized third-party.

75. By collecting, storing, sharing, and using the Plaintiff's and Class Members' PII for commercial gain, Defendant assumed a duty to use reasonable means to safeguard the personal data it obtained.

76. Defendant is a financial institution and has a duty to develop, implement, and maintain a written information security program designed to protect customer information. The information security program must be appropriate to the size and complexity of the business, the nature and scope of business activities, and the sensitivity of the information at issue.

77. Defendant's information security program must be designed to: (a) ensure the security and confidentiality of customer information; (b) protect against anticipated threats or hazards to the security or integrity of that information; and (c) protect against unauthorized access to that information that could result in substantial harm or inconvenience to any customer.

78. Defendant's duty included a responsibility to ensure it: (i) implemented reasonable administrative, technical, and physical measures to detect and prevent unauthorized intrusions into its information technology and/or cloud environments; (ii) contractually obligated its vendors to adhere to the requirements of Defendant's privacy policy; (iii) complied with the Safeguards Rule and other applicable statutes and data protection obligations; (iv) conducted regular privacy assessments and security audits of Defendant's and/or its vendors' data processing activities; (v) regularly audited for compliance with contractual and other applicable data protection obligations; and, (vi) provided timely notice to individuals impacted by a data breach event.

79. Defendant also 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 or deceptive trade practices that affect commerce. Deceptive practices, as interpreted by the FTC, include failing to adhere to a company's own published privacy policies.

80. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII that Defendant was no longer required to retain.

81. Defendant had a duty to notify Plaintiff and the Classes of the Data Breach promptly and adequately. Such notice was necessary to allow Plaintiff and

the Classes to take steps to prevent, mitigate, and repair any fraudulent usage of their PII.

82. Defendant violated Section 5 of the FTC Act by failing to adhere to its own privacy policy[15] regarding the confidentiality and security of Plaintiff and Class Members information. Defendant further violated Section 5 of the FTC Act, the Safeguards Rule, and other state consumer protection statutes by failing to implement an information security plan or use reasonable security measures to protect PII. Defendant's violations of Section 5 of the FTC Act, the Safeguards Rule, and other state consumer protection statutes, constitutes negligence *per se*.

83. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant includes, but are not limited to, the following:

a. Failing to designate a qualified individual to implement and supervise its information security program.

b. Failing to conduct an assessment to determine foreseeable risks and threats – internal and external – to the security, confidentiality, and integrity of customer information.

c. Failing to design and implement safeguards to control the risks identified through the risk assessment.

d. Failing to implement organizational controls, including a patch management policy to track and manage updates and patches for known vulnerabilities.

[15] https://www.firstcomcu.org/privacypolicy.html.

e. Failing to have defined periods when patches must be installed and/or an automated means of determining what patches are needed, where they are needed, and the status of current patch levels by location.

f. Failing to encrypt personally identifying information in transit and at rest.

g. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII.

h. Failing to adequately monitor the security of their networks and systems.

i. Allowing unauthorized access to PII.

j. Failing to detect in a timely manner that PII had been compromised.

k. Failing to remove former customers' PII it was no longer required to retain.

l. Failing to timely and adequately notify Plaintiff and 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.

m. Failing to implement data security practices consistent with Defendant's published privacy policies.

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

85. The injuries resulting to Plaintiff and the Classes because of Defendant's failure to use adequate security measures were reasonably foreseeable.

86. Plaintiff and the Classes were the foreseeable victims of a data breach. Defendant knew or should have known of the inherent risks in collecting and storing

PII, the critical importance of protecting that PII, and the necessity of updating, patching, or fixing critical vulnerabilities in its network.

87. Plaintiff and the Classes had no ability to protect the PII in Defendant's possession. Defendant was in the best position to protect against the harms suffered by Plaintiff and the Classes as a result of the Data Breach.

88. But for Defendant's breach of duties owed to Plaintiff and the Classes, their PII would not have been compromised. There is a close causal connection between Defendant's failure to implement reasonable security measures to protect the PII of Plaintiff and the Classes and the harm, or risk of imminent harm, suffered by Plaintiff and the Classes.

89. As a result of the Data Breach, Plaintiff and Class Members suffered injuries 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) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized

disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PII.

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

91. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to: (i) strengthen its data protection procedures; (ii) patch all critical vulnerabilities; and (iii) to provide adequate credit monitoring to all affected by the Data Breach.

COUNT 2: BREACH OF IMPLIED CONTRACT

92. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

93. Defendant requires their customers, including Plaintiff and Class Members, to submit PII in the ordinary course of providing products or services.

94. Defendant published a privacy policy to inform the public about how Defendant collects, uses, shares, and protects the information Defendant gathers in connection with the provision of those products or services.

95. In so doing, Plaintiff and Class Members entered implied contracts with Defendant by which Defendant agreed to use reasonable technical, administrative, and physical safeguards to protect against unauthorized access to, use of, or disclosure of the personal information it collects and stores.

96. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of an expressed or implied promise to implement reasonable data protection measures.

97. Plaintiff and Class Members fully and adequately performed their obligations under the implied contract with Defendant.

98. Defendant breached the implied contract with Plaintiff and Class Members which arose from the course of conduct between the parties, as well as disclosures on the Defendant's web site, privacy policy, and in other documents, all of which created a reasonable expectation that the personal information Defendant collected would be adequately protected and that the Defendant would take such actions as were necessary to prevent unauthorized access to, use of, or disclosure of such information.

99. As a direct and proximate result of the Defendant's breach of an implied contract, Plaintiff and Class Members suffered injuries 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) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to

access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PII.

100. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to: (i) strengthen its data protection procedures; (ii) patch all critical vulnerabilities; and (iii) to provide adequate credit monitoring to all affected by the Data Breach.

COUNT 3: UNJUST ENRICHMENT

101. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

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

103. By providing their PII, Plaintiff and Class Members conferred a monetary benefit on Defendant. Defendant used the PII to market, advertise, and sell additional services to Plaintiff and Class Members. Defendant knew that Plaintiff and Class Members conferred a benefit upon them and have accepted and retained that benefit.

104. By collecting the PII, Defendant was obligated to safeguard and protect such information, to keep such information confidential, and to timely and

accurately notify Plaintiff and Class Members if their data had been compromised or stolen.

105. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, it would be unjust for Defendant to retain any of the benefits that Plaintiff and Class Members conferred upon Defendant without paying value in return.

106. As a direct and proximate result of the Defendant's conduct, Plaintiff and Class Members suffered injuries 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) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PII.

107. 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.

COUNT 4: INVASION OF PRIVACY

108. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

109. Plaintiff and Class Members had a legitimate expectation of privacy in their personally identifying information such as Social Security numbers, dates of birth, and financial account numbers. Plaintiff and Class Members were entitled to the protection of this information from disclosure to unauthorized third parties.

110. Defendant owed a duty to Plaintiff and Class Members to keep their PII confidential.

111. Defendant permitted the public disclosure of Plaintiff's and Class Members' PII to unauthorized third parties.

112. The PII that was disclosed without the Plaintiff's and Class Members' authorization was highly sensitive, private, and confidential. The public disclosure of the type of PII at issue here would be highly offensive to a reasonable person of ordinary sensibilities.

113. Defendant permitted its information technology environment to remain vulnerable to foreseeable threats, which created an atmosphere for the Data Breach to occur. Despite knowledge of the substantial risk of harm created by these conditions, Defendant intentionally disregarded the risk, thus permitting the Data Breach to occur.

114. By permitting the unauthorized disclosure, Defendant acted with reckless disregard for the Plaintiff's and Class Members' privacy, and with knowledge that such disclosure would be highly offensive to a reasonable person. Furthermore, the disclosure of the PII at issue was not newsworthy or of any service to the public interest.

115. Defendant was aware of the potential of a data breach and failed to adequately safeguard its systems and/or implement appropriate policies and procedures to prevent the unauthorized disclosure of Plaintiff's and Class Members' data.

116. Defendant acted with such reckless disregard as to the safety of Plaintiff's and Class Members' PII to rise to the level of intentionally allowing the intrusion upon the seclusion, private affairs, or concerns of Plaintiff and Class Members.

117. Plaintiff and Class Members have been damaged by the invasion of their privacy in an amount to be determined at trial.

COUNT 5: VIOLATION OF PENNSYLVANIA'S UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW
{73 P.S. §§201-*1 et seq*.}

118. Plaintiff re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

119. Plaintiff and Class Members are consumers of Defendant's products

and services. Defendant requires its customers, including Plaintiff and Class Members, to submit PII in the ordinary course of providing products or services.

120. Defendant gathered and stored the PII of Plaintiff and Class Members as part of its business of soliciting its services to customers. Plaintiff and Class Members entrusted Defendant with their PII with the understanding that Defendant would adequately safeguard their information.

121. Under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits unfair or deceptive trade practices that affect commerce. Deceptive practices, as interpreted by the FTC, include failing to adhere to a company's own published privacy policies. Such behavior by Defendant also constitutes a false, misleading, or deceptive act under Pennsylvania's Unfair Trade Practices and Consumer Protection Law.

122. Defendant violated the state consumer protection statute by failing to adhere to its own Privacy Policy regarding the confidentiality and security of Plaintiff's and Class Members' information. Defendant further violated the state consumer protection statute by failing to use reasonable measures to protect PII.

123. Defendant's conduct created a likelihood of confusion or misunderstanding regarding its actual data privacy and security practices. Defendant promised to protect Plaintiff's and Class Members' PII via its privacy policies, but allowed the unauthorized access to this personal and protected health

information; Defendant failed to disclose material facts that the Plaintiff's and Class Members' PII would be disclosed to unauthorized third parties; Defendant failed to obtain Plaintiff's and Class Members' consent in transmitting their PII to a third party; and knowingly violated industry and legal standards regarding the protection of Plaintiff's and Class Members' PII.

124. Defendant's unfair or deceptive acts affected public interests, including those of Plaintiff and Class Members. Defendant knew or should have known that it was likely to mislead its customers who were acting reasonably. Defendant engaged in unfair or deceptive practices by breaching its duties to provide technical and organizational data security policies, procedures, and practices. Defendant's failure to adhere to its published privacy policies and procedures is offensive to established public policy and is substantially injurious to consumers as evidenced by the massive Data Breach.

125. Had Plaintiff and Class Members known Defendant would not follow its own published security practices they would not have purchased (or continued to purchase) Defendant's products or services. Defendant's deceptive acts, as described herein, proximately caused Plaintiff and Class Members damages.

126. As a direct and proximate result of the Defendant's conduct, Plaintiff and Class Members suffered 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) mitigation costs and expenses; (vii) statutory damages; and (viii) attorneys' fees and court costs.

127. Plaintiff alleges that Defendant's data security measures remain inadequate. Plaintiff will continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

128. Plaintiff and Class Members have suffered irreparable injury, and will continue to suffer injury in the future, as a result of Defendant's deceptive trade practices, which places Plaintiff and Class Members at imminent risk that further compromises of their PII will occur in the future. As such, the remedies available at law are inadequate to compensate for that injury. Accordingly, Plaintiff and Class Members also seek to obtain a judgment declaring, among other things, the following:

a. Defendant continues to owe a legal duty to secure PII and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes.

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiff and Class Members' PII.

129. The Court also should issue corresponding prospective injunctive relief requiring that Defendant employs adequate data protection practices consistent with law and industry standards.

130. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Among other things, if another massive data breach occurs, Plaintiff will likely be subjected to fraud, identity theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

131. The issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by encouraging Defendant to take necessary action to prevent another data breach, thus eliminating the additional injuries that would result to Plaintiff and the multitude of individuals whose PII would be at risk of future unauthorized disclosures.

132. As a result of the Defendant's false, misleading, or deceptive acts, regarding its data security practices, the consuming public in general, Plaintiff, and Class Members suffered injuries including, but not limited to, the future and continued risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to

protect the PII.

133. Plaintiff and Class Members are entitled to statutory damages, attorneys' fees, costs, and injunctive relief requiring Defendant to: (i) strengthen its data protection procedures; (ii) implement strong authentication mechanisms for accessing cloud services; and (iii) to provide adequate dark web monitoring and/or credit monitoring to all affected by the Data Breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Classes alleged herein, respectfully requests that the Court enter judgment as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff(s) as the representatives for the Classes and counsel for Plaintiff(s) as Class Counsel;

B. For an order declaring the Defendant's conduct violates the statutes and causes of action referenced herein;

C. For an order finding in favor of Plaintiff and the Classes on all counts asserted herein;

D. Ordering Defendant to pay for lifetime credit monitoring and dark web scanning services for Plaintiff and the Classes;

E. For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;

F. For prejudgment interest on all amounts awarded;

G. For an order of restitution and all other forms of equitable monetary relief requiring the disgorgement of the revenues wrongfully retained as a result of the Defendant's conduct;

H. For injunctive relief as pleaded or as the Court may deem proper; and

I. For an order awarding Plaintiff and the Classes their reasonable attorneys' fees and expenses and costs of suit, and any other expense, including expert witness fees; and

J. Such other relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of all claims in this Complaint and of all issues in this action so triable as of right.

Dated: Thursday, August 21, 2024.

By: */s/ Stuart Guber*
Stuart Guber, Esq. Bar: 60772
Paul J. Doolittle, Esq.*
POULIN | WILLEY | ANASTOPOULO
32 Ann Street
Charleston, SC 29403
Telephone: (803) 222-2222
Fax: (843) 494-5536
Email: stuart.guber@poulinwilley.com
paul.doolittle@poulinwilley.com
cmad@poulinwilley.com

Attorneys for Plaintiff
**Pro Hac Vice forthcoming*

JS 44 (Rev. 04/21)

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.)*

I. (a) PLAINTIFFS

Joshua Ambrose-Manness

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Stuart Guber, Poulin Willey Anastopoulo, 32 Ann Street, Charleston, SC 29403 (803)222-2222

DEFENDANTS

First Commonwealth Federal Credit Union

County of Residence of First Listed Defendant Lehigh County
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

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

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 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)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☒ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

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

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

INTELLECTUAL PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 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)***:
CAFA 28 U.S.C. 1332(d)

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+

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE 08/21/2024

SIGNATURE OF ATTORNEY OF RECORD /s/ Stuart Guber

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

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 cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

DESIGNATION FORM
(to be used by counsel to indicate the category of the case for the purpose of assignment to the appropriate calendar)

Address of Plaintiff: 231 West Columbus Avenue, APT 1, Nesquehoning, PA 18240

Address of Defendant: 6126 Hamilton Boulevard, Suite 100, Allentown, Lehigh County, Pennsylvania 18106.

Place of Accident, Incident or Transaction: 6126 Hamilton Boulevard, Suite 100, Allentown, Lehigh County, Pennsylvania 18106.

RELATED CASE IF ANY:
Case Number:_____ Judge:_____ Date Terminated_____

Civil cases are deemed related when ***Yes*** is answered to any of the following questions:

1. Is this case related to property included in an earlier numbered suit pending or within one year previously terminated action in this court? Yes ☐ No ☒ X
2. Does this case involve the same issue of fact or grow out of the same transaction as a prior suit Pending or within one year previously terminated action in this court? Yes ☐ No ☒ X
3. Does this case involve the validity or infringement of a patent already in suit or any earlier Numbered case pending or within one year previously terminated action of this court? Yes ☐ No ☒ X
4. Is this case a second or successive habeas corpus, social security appeal, or pro se case filed by the same individual? Yes ☐ No ☒ X

I certify that, to my knowledge, the within case ☐ **is** / ☑ **is not** related to any now pending or within one year previously terminated action in this court except as note above.

DATE: 8/21/2024 /s/ Stuart Guber 60772

Attorney-at-Law (Must sign above) *Attorney I.D. # (if applicable)*

Civil (Place a √ in one category only)

A. Federal Question Cases:

- ☐ 1. Indemnity Contract, Marine Contract, and All Other Contracts)
- ☐ 2. FELA
- ☐ 3. Jones Act-Personal Injury
- ☐ 4. Antitrust
- ☐ 5. Wage and Hour Class Action/Collective Action
- ☐ 6. Patent
- ☐ 7. Copyright/Trademark
- ☐ 8. Employment
- ☐ 9. Labor-Management Relations
- ☐ 10. Civil Rights
- ☐ 11. Habeas Corpus
- ☐ 12. Securities Cases
- ☐ 13. Social Security Review Cases
- ☐ 14. Qui Tam Cases
- ☐ 15. All Other Federal Question Cases. *(Please specify)*:_____

B. Diversity Jurisdiction Cases:

- ☐ 1. Insurance Contract and Other Contracts
- ☐ 2. Airplane Personal Injury
- ☐ 3. Assault, Defamation
- ☐ 4. Marine Personal Injury
- ☐ 5. Motor Vehicle Personal Injury
- ☐ 6. Other Personal Injury (*Please specify*):_____
- ☐ 7. Products Liability
- ☒ X 8. All Other Diversity Cases: *(Please specify)* data breach

ARBITRATION CERTIFICATION
(The effect of this certification is to remove the case from eligibility for arbitration)

I, Stuart Guber, counsel of record *or* pro se plaintiff, do hereby certify:

- ☒ X Pursuant to Local Civil Rule 53.2 § 3(c)(2), that to the best of my knowledge and belief, the damages recoverable in this civil action case exceed the sum of $150,000.00 exclusive of interest and costs:
- ☒ X Relief other than monetary damages is sought.

DATE: 8/21/2024 /s/ Stuart Guber 60772

Attorney-at-Law (Sign here if applicable) *Attorney ID # (if applicable)*

NOTE: A trial de novo will be a jury only if there has been compliance with F.R.C.P. 38.