UNITED STATES DISTRICT COURT
DISTRICT OF COLORADO

Maritza Rodriguez, *et al.* **Plaintiff,** **v.** **Professional Finance Company, Inc.,** **Defendant.**	Case No. 1:22-cv-01679-RMR-STV Judge Regina M. Rodriguez JURY TRIAL DEMANDED

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Maritza Rodriguez, Jerry Blake, Natalie Willingham, Christopher Schroeder, Ryan McGarrigle, and Marko Skrabo (collectively "Plaintiffs") bring this Consolidated Class Action Complaint against Professional Finance Company, Inc. ("PFC" or "Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and allege, upon personal knowledge as to their own actions and their counsel's investigations, and upon information and belief as to all other matters, as follows:

1. Defendant PFC is a large accounts receivable management company with its primary place of business located in Greeley, Colorado. As part of Defendant's business, it acquires, stores, processes, analyzes, and otherwise utilizes for its business purposes personally identifiable information ("PII"), including first and last names, dates of birth, addresses, accounts receivable balances, information regarding payments made to accounts, and Social Security numbers, as well as protected health information ("PHI"), including health insurance and medical treatment information (collectively, PII and PHI are "Private Information").

2. Plaintiffs and Class Members are individuals whose Private Information was acquired, stored, and utilized by Defendant for its business and financial benefit.

3. By obtaining, collecting, utilizing, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant owed and otherwise assumed statutory, regulatory, contractual, and common law duties and obligations to keep Plaintiffs' and Class Members' Private Information confidential, safe, secure, and protected from the unauthorized access, disclosure, and theft in foreseeable data breach incidents.

4. Defendant, however, disregarded its duties and obligations and the privacy rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable data security measures to protect and safeguard the Private Information of Plaintiffs and Class Members, by allowing the Private Information to be stored and maintained in a vulnerable state.

5. As a result of Defendant's failure to implement and maintain reasonable data security measures, a group of well-known cybercriminals, using well-known attack methods, were able to target, access, exfiltrate, and steal the Private Information of Plaintiffs and nearly two million other Class Members (the "Data Breach"). But for Defendant's acts and omissions, the Data Breach would not have happened, and Plaintiffs and Class Members would not have been injured as described herein.

6. Defendant admits on its various notice letters to Plaintiffs and the Class Members that the unencrypted Private Information impacted during the Data Breach included names, addresses, dates of birth, Social Security numbers, medical information, and health insurance information.

7. The exposed Private Information of Plaintiffs and Class Members is highly sensitive and can be utilized to commit identity theft and fraud. Plaintiffs' and Class Members' Private Information has been or likely will be sold on the dark web, as this is the *modus operandi* for cyber criminals targeting this type of Private Information. Plaintiffs and Class Members, therefore, are now at a substantial current and ongoing risk of identity theft, which is heightened here by the loss of Social Security numbers – the gold standard for identity thieves.

8. While many details of the Data Breach remain in the exclusive control of Defendant, upon information and belief, Defendant breached its duties and obligations by failing to, in one or more of the following ways: (1) design, implement and maintain reasonable network safeguards against foreseeable threats; (2) design, implement, and maintain reasonable data retention policies; (3) adequately train employees on data security; (4) comply with industry-standard data security practices; (5) warn Plaintiffs and Class Members of Defendant's inadequate data security practices; (6) encrypt or adequately encrypt the Private Information; (7) recognize or detect that Conti, a ransomware organization, had accessed its network in a timely manner to mitigate the harm; (8) utilize widely available software able to detect and prevent Conti ransomware, and (9) otherwise secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

9. Moreover, despite learning of the Data Breach in February 2022, Defendant did not begin notifying its healthcare provider clients, Plaintiffs, and Class Members until approximately July 2022. Defendant delayed sending notice of the Data Breach even though it was aware of the need to move quickly in responding to Data Breach events due to the nature of its business and the sensitive information it maintains on Plaintiffs and Class Members.

10. As a result of Defendant's acts and omissions, Plaintiffs and Class Members had their most sensitive Private Information stolen by malicious cybercriminals. The information that was compromised is a one-stop shop for identity thieves to wreak havoc on Plaintiffs' and Class Members' personal and financial lives. Given the sensitivity and static nature of the information involved (such as names, Social Security numbers, and dates of birth), the risk of identity theft is present, materialized, and will continue into the foreseeable future for Plaintiffs and Class Members. Plaintiffs and Class Members will therefore now live with the present and ongoing risk of identity theft, which will require third-party professional services to monitor their Private Information for criminal misuse and dark web activity.

11. As a direct result of the Data Breach, Plaintiffs and Class Members have suffered the following actual and imminent injuries: (i) invasion of privacy; (ii) out-of-pocket expenses; (iii) loss-of time and productivity incurred mitigating the present risk and imminent threat of identity theft; (iv) actual identity theft and fraud resulting in additional economic and non-economic damages; (v) diminution of value of their Private Information; (vi) anxiety, stress, nuisance, and annoyance; (vii) increased targeted and fraudulent robocalls and phishing email attempts; (viii) the present and continuing risk of identity theft posed by their Private Information being placed in the hands of the ill-intentioned hackers and/or criminals; (ix) the retention of the reasonable value of the Private Information entrusted to Defendant; and (x) the present and continued risk to Private Information, which remains on Defendant's vulnerable network, placing Plaintiffs and Class Members at an ongoing risk of harm.

12. Plaintiffs bring this class action to remedy these harms, on behalf of themselves and all similarly situated persons whose Private Information was compromised in the Data Breach. Plaintiffs seek compensatory damages, incidental damages, and consequential damages for the

diminution in value of their Private Information, invasion of their privacy, loss of their time, loss of their productivity, out-of-pocket costs, and future costs of necessary identity theft monitoring. Plaintiffs also seek injunctive relief including improvements to Defendant's data security system and protocols, deletion of Private Information that is unnecessary for legitimate business purposes, and future annual audits to protect their Private Information against foreseeable future cyber security incidents.

13. Plaintiffs bring this Consolidated Class Action Complaint against Defendant asserting claims for: (1) negligence, (2) breach of implied contract, (3) breach of third party beneficiary contract, (4) unjust enrichment, (5) invasion of privacy, (6) violations of the Colorado Consumer Protection Act, Colo. Rev. Stat. § 6-1-101, *et seq.*, (7) violations of the Arizona Consumer Fraud Act, Ariz. Rev. Stat. § 44-1521, *et seq.*, (8) violations of the California Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*, (9) violations of the California Unfair Competition Law, Cal. Bus. Code §17200, *et seq.*, (10) violations of the California Consumer Privacy Act, Cal. Civ. Code § 1798.150, (11) violations of Nevada Consumer Fraud Act, Nev. Rev. Stat. §§ 598.0915 and 598.0923, *et seq.*, and (12) declaratory judgment/injunctive relief.

PARTIES

Plaintiff Jerry Blake

14. Plaintiff Jerry Blake is a resident and citizen of Mississippi, residing in Ackerman, Mississippi.

15. Plaintiff Blake received a letter dated July 1, 2022, from Defendant PFC concerning the Data Breach. The letter stated that unauthorized actors gained access to files on PFC's network. The compromised files contained Plaintiff Blake's Private Information.

Plaintiff Ryan McGarrigle

16. Plaintiff Ryan McGarrigle is a resident and citizen of California, residing in Chula Vista, California.

17. Plaintiff McGarrigle received a letter dated July 1, 2022, from Defendant PFC concerning the Data Breach. The letter stated that unauthorized actors gained access to files on PFC's network. The compromised files contained Plaintiff McGarrigle's Private Information.

Plaintiff Maritza Rodriguez

18. Plaintiff Maritza Rodriguez is a resident and citizen of Arizona, residing in Tucson, Arizona.

19. Plaintiff Rodriguez received a letter dated July 1, 2022, from Defendant PFC concerning the Data Breach. The letter stated that unauthorized actors gained access to files on PFC's network. The compromised files contained Plaintiff Rodriguez's Private Information.

Plaintiff Christopher Schroeder

20. Plaintiff Christopher Schroeder is a resident and citizen of Nevada, residing in Reno, Nevada.

21. Plaintiff Schroeder received a letter dated July 1, 2022, from Defendant PFC concerning the Data Breach. The letter stated that unauthorized actors gained access to files on PFC's network. The compromised files contained Plaintiff Schroeder's Private Information.

Plaintiff Marko Skrabo

22. Plaintiff Marko Skrabo is a resident and citizen of Colorado, residing in Parker, Colorado.

23. Plaintiff Skrabo received a letter dated July 1, 2022, from Defendant PFC concerning the Data Breach. The letter stated that unauthorized actors gained access to files on PFC's network. The compromised files contained Plaintiff Skrabo's Private Information.

Plaintiff Natalie Willingham

24. Plaintiff Natalie Willingham is a resident and citizen of Texas, residing in Hayes County, Texas.

25. Plaintiff Willingham received a letter dated July 1, 2022, from Defendant PFC concerning the Data Breach. The letter stated that unauthorized actors gained access to files on PFC's network. The compromised files contained Plaintiff Willingham's Private Information.

Defendant Professional Finance Company, Inc.

26. Defendant Professional Finance Company, Inc. is a corporation organized under the laws of Colorado, and its United States headquarters and principal place of business is located at 5754 W. 11th St., Ste 100, Greeley, Colorado 80634.

JURISDICTION AND VENUE

27. 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 some Plaintiffs, are citizens of a state different from Defendant.

28. 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 Plaintiffs' claims occurred in and emanated from this District.

29. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

FACTUAL ALLEGATIONS

30. Defendant PFC boasts that it is one of the nation's leading debt recovery agencies, serving clients throughout the country in the healthcare, retail, finance, and governmental services industries.[1] Defendant's website further states that "[t]housands of national clients rely on [Defendant] to recover their receivables and manage their early out self-pay programs."[2]

Defendant Collects Private Information

31. Defendant collects the Private Information of its clients' customers as a condition of providing services. This Private Information is used by Defendant in the ordinary course of its business to, *inter alia*, collect debts from medical patients. At the time of the Data Breach, Defendant provided services to approximately 657 different healthcare organizations.

32. The types of private information collected and utilized by PFC include, full names, dates of birth, social security numbers, phone numbers, addresses, email addresses, account numbers, original creditors, current creditors, balance, and payment histories, health insurance information, and medical treatment information.

Defendant's Privacy Policy & Promises

33. On its customer-facing website, Defendant has a posted Privacy Policy, last updated February 25, 2020 (the "Privacy Policy").[3]

[1] https://www.hipaajournal.com/657-healthcare-providers-affected-by-ransomware-attack-on-professional-finance-company/ (last visited: July 7, 2022).
[2] https://www.pfcusa.com/about-us/ (last visited: July 6, 2022).
[3] https://www.pfcusa.com/privacy-policy/ (last visited July 6, 2022).

34. Defendant's Privacy Policy acknowledges that Defendant has a duty to protect Plaintiffs' and Class Members' Private Information.[4]

35. Defendant's Privacy Policy pertains to Private Information provided to Defendant and any Private Information that Defendant collects.[5]

36. The Privacy Policy states "[y]our privacy is important to PFC. Our Privacy Policy covers how PFC collects, uses, maintains and discloses your personal information."[6]

37. The Privacy Policy also discusses the types of information PFC collects and the reasons that it might use that information. It states, in part:

> In order to provide and improve our services, we collect personal information. Most of the information we have is provided to us by the creditor and/or collected directly through the use of our services, emails, web applications, and phone calls.
>
> Here are some examples of the types of personal information PFC may collect and how we use it:
>
> - When an account is transferred to PFC the creditor provides a variety of information which may include, but is not limited to: full name, date of birth, social security number, phone number, address, email address, account number, original creditor, current creditor, balance, payment history.
>
> - We may collect any information that you provide to us directly whether you contact us by phone, email, sms, web applications, or any other channel. For example, when you access PFC web applications and fill out a form or sign up for a payment plan and provide information such as your first and last name, email address, mailing address, phone number, credit card information and/or other personal identifying information.
>
> - When you access PFC emails or our web applications we may collect a variety of information and store it in log files, including, but not limited to Internet Protocol (IP) address, browser type and language, Internet service provider (ISP), type of computer, operating system, date/time stamp, user interface interaction data (such as, but not limited to, any mouse clicks or navigation on our emails and web applications), uniform resource locator

[4] https://www.pfcusa.com/privacy-policy/ (last visited July 6, 2022).
[5] *Id.*
[6] *Id.*

> (URL) information (showing where you came from or where you go to next), email open rates, credit card, bank account information.
>
> ***Using Personal Information***
>
> We use personal information to properly identify the specific consumers for whom we provide our services, to provide and improve our services, to analyze trends, administer our web applications, learn about user behavior on our emails and web applications, to comply with state, federal and local laws and to demonstrate compliance with those laws.

38. The Privacy Policy also provides instances when PFC might share PII and PHI with third parties. It states:

> We only share personal information with a limited number of third party service providers who help us provide our services, including, but not limited to, payment processing, mailing, information verification, managing and enhancing customer data, improving our product and services. When we share information, we require those third parties to handle it in accordance with relevant laws. We also only share the minimum amount of information necessary for the particular third party to assist us in providing our service.[7]

39. Defendant lists a number of instances when it might share or disclose the Private Information entrusted to it without permission, none of which are applicable here.[8]

40. The Privacy Policy also states, under *Integrity and Retention of Personal Information*, that "PFC will retain your personal information for the period required to fulfill our services, meet our contractual obligations, and as required by law."

41. Further, under *How We Protect Your Information*, Defendant states "PFC is serious about data security."[9] With respect to the data stored on its systems, Defendant states:

> We seek to implement the best practices in data collection, storage, processing, and security to protect against unauthorized access and disclosure. PFC protects your personal information during transit using encryption such as Transport Layer Security (TLS) and at rest using encryption such as AES 256. When your personal data is stored by PFC, we

[7] *Id.*
[8] *See id.*
[9] *Id.*

> use computer systems with limited access housed in facilities using physical security measures.[10]

42. Finally, Defendant's payment portal, accessible through its debt collection website "pfccollects.com" has a "Privacy Policy."[11] It states, in part:

> Professional Finance Company has created this security and privacy statement in order to document and communicate its commitment to doing business with the highest ethical standards and appropriate internal controls. This Internet Privacy Policy describes the privacy policies applicable to Professional Finance Company's U.S. Internet websites www.ProfessionalFinanceCompany.com, www.pfccollects.com, and www.paypfc.com. Professional Finance Company has implemented physical, electronic, and procedural security safeguards to protect against the unauthorized release of or access to personal information. To further safeguard this information, our employees are asked to sign an acknowledgment of Professional Finance Company's Standards of Employee Conduct, which includes the Company Equipment and Office Guidelines and the General Technology Use Guidelines. Employees are subject to disciplinary action up to and including termination of employment if they fail to follow signed acknowledgments.[12]

43. It also states that to access the Defendant's website for "purposes of reviewing an account or making payment to PFC, personally identifiable information (PII) *must be provided*."[13] It continues to state that the types of "PII that may be collected includes: (1) A first and last name. (2) A home or other physical address, including street name and name of a city or town. (3) An e-mail address. (4) A telephone number. (5) A social security number. (6) A date of birth. (7) An employer. (8) A spouse's name and contact information."[14]

---

[10] *Id.*
[11] The Payment Portal Privacy Policy is no longer available, however, a web-archived snapshot dated March 29, 2019 is available at https://web.archive.org/web/20190329055426/https://pfccollects.com/p/privacy-policy.html (last visited July 7, 2022).
[12] *Id.*
[13] *Id.* (emphasis added).
[14] *Id.*

The Data Breach

44. According to PFC, on February 26, 2022, it detected a ransomware attack in which "an unauthorized third party accessed and disabled some of PFC's computer systems."[15]

45. According to PFC, its subsequent investigation "determined that an unauthorized third party accessed files containing certain individuals' personal information during this incident."[16] It has been publicly reported the "unauthorized third party" who executed the Data Breach is "linked to Conti/Quantum ransomware sub-group."[17]

46. PFC has confirmed that highly sensitive categories of PII and PHI were exposed in the Breach, including but not limited to, the following: first and last names, dates of birth, addresses, accounts receivable balances and information regarding payments made to accounts, Social Security numbers, and health insurance and medical treatment information.[18]

47. Defendant sent Plaintiffs and Class Members a Notice of Data Security Incident letter on or around July 1, 2022. The Notice of Data Security Incident letter informed Plaintiffs and Class Members as follows:

> On February 26, 2022, PFC detected and stopped a sophisticated ransomware attack in which an unauthorized third party accessed and disabled some of PFC's computer systems. PFC immediately engaged third party forensic specialists to assist us with securing the network environment and investigating the extent of any unauthorized activity. Federal law enforcement was also notified. The ongoing investigation determined that an unauthorized third party accessed files containing certain individuals' personal information during this incident. PFC notified the respective healthcare providers on or around May 5, 2022. This incident only impacted data on PFC's systems. The list of healthcare providers can be viewed here: https://bit.ly/CoveredEntitiesPFC PFC found no evidence that personal

[15] https://www.prnewswire.com/news-releases/pfc-usa-provides-notice-of-data-security-incident-301579798.html (last visited Oct. 25, 2022).
[16] https://www.prnewswire.com/news-releases/pfc-usa-provides-notice-of-data-security-incident-301579798.html (last visited Oct. 25, 2022).
[17] https://www.bleepingcomputer.com/news/security/quantum-ransomware-attack-affects-657-healthcare-orgs/ (last visited Oct. 25, 2022).
[18] https://www.prnewswire.com/news-releases/pfc-usa-provides-notice-of-data-security-incident-301579798.html (last visited Oct. 25, 2022).

> information has been specifically misused; however, it is possible that the following information could have been accessed by an unauthorized third party: first and last name, address, accounts receivable balance and information regarding payments made to accounts, and, in some cases, date of birth, Social Security number, and health insurance and medical treatment information.

48. PFC reported to the U.S. Department of Health and Human Services Office for Civil Rights that the Data Breach impacted the Private Information of at least 1,918,941 individuals. PFC has also published a list of 657 healthcare clients with patients whose Private Information was compromised as a result of the Data Breach.[19]

49. Following the Data Breach, PFC instructed Plaintiffs and Class Members to "remain vigilant to protect against fraud and/or identity theft by, among other things, reviewing their financial account statements and monitoring free credit reports."[20]

50. PFC reprehensibly downplayed the risk faced by Plaintiffs and Class Members by publicly stating that, "PFC found no evidence that personal information has been specifically misused . . . ." Of course, the same notice states that if victims do experience fraud, they should not contact PFC, but should instead "promptly notify the institution or company with which the account is maintained" or "proper law enforcement authorities . . . ." Thus, whether PFC itself is aware of misuse is both misleading and irrelevant because PFC expressly instructs victims of the Data Breach not to contact it regarding instances of fraud.

51. Defendant also inexcusably omitted in notice letters to Plaintiffs and Class Members that the perpetrator of the attack was Quantum Locker, a splinter cell of the notorious

[19] The list can be found at: https://dta0yqvfnusiq.cloudfront.net/pfcco40463296/2022/07/Website-Covered-Entities-Final-7-18-22-62d5ccc53001c.pdf (last visited Oct. 25, 2022).

[20] https://www.prnewswire.com/news-releases/pfc-usa-provides-notice-of-data-security-incident-301579798.html (last visited Oct. 25, 2022).

Conti crime syndicate, known to sell Private Information on the dark web following similar ransomware attacks.

Quantum Locker

52. "Discovered in August 2021, Quantum ransomware is linked to the Quantum Locker operation. Quantum Locker has had a few rebrands (AstroLocker, MountLocker, and XingLocker)."[21]

53. Around the time of the Data Breach, Quantum came under control of a splinter group from the notorious Conti ransomware organization.[22] Conti is responsible for hundreds of widely publicized cyberattacks over the past two years.

54. The specifics of Quantum's attack practices before and after the merger with Conti are well documented.[23]

55. Despite the sophistication of Quantum's attack profile, it must rely on rudimentary social engineering techniques like phishing to deploy malware and initiate an attack.[24] "Although Quantum now uses call-back phishing, they have also used email phishing in their social engineering attacks."[25] Both methods of phishing are detectable and preventable through the use of proper threat detection software, employee training, and required two-factor or multi-factor authentication to access accounts or systems.

[21] https://www.avertium.com/resources/threat-reports/an-in-depth-look-at-quantum-ransomware (last visited Oct. 30, 2022).
[22] *Id.*
[23] A step-by-step breakdown of the process can be found at: https://www.cybereason.com/blog/cybereason-vs.-quantum-locker-ransomware (last visited Oct. 25, 2022); *see also* https://www.avertium.com/resources/threat-reports/an-in-depth-look-at-quantum-ransomware (last visited Oct. 30, 2022).
[24] https://www.cybereason.com/blog/cybereason-vs.-quantum-locker-ransomware (last visited Oct. 25, 2022).
[25] https://www.avertium.com/resources/threat-reports/an-in-depth-look-at-quantum-ransomware (last visited Oct. 30, 2022).

56. Through a successful phishing campaign, Quantum typically injects IcedID malware and a LNK shortcut to execute it. IcedID is a modular banking trojan used for the past five years, primarily for second-stage payload deployment, loaders, and ransomware.[26]

57. After successfully injecting its malware, Quantum deploys Cobalt Strike and RDP to move across the network encrypting and stealing sensitive data to hold for ransom.[27]

58. After data has been stolen, Quantum attempts to sell it back to the company it stole it from. However, if the company refuses to pay the ransom, Quantum sells the information to other cybercriminals on the dark web.

The Data Breach was Foreseeable and Preventable

59. Ransomware attacks, like that experienced by Defendant, are a well-known threat to companies that maintain Private Information. Companies should treat ransomware attacks as any other data breach incident because ransomware attacks don't just hold networks hostage; through a ransomware attack, the cybercriminal accesses the data and captures it. "[R]ansomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[28] As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence […] the initial assumption should be that data may have been exfiltrated."

60. An increasingly prevalent form of ransomware attack is the "encryption+exfiltration" attack in which the attacker encrypts a network and exfiltrates the data

[26] https://www.bleepingcomputer.com/news/security/quantum-ransomware-seen-deployed-in-rapid-network-attacks/ (last visited Oct. 30, 2022).
[27] https://www.avertium.com/resources/threat-reports/an-in-depth-look-at-quantum-ransomware (last visited Oct. 30, 2022).
[28] *Ransomware: The Data Exfiltration and Double Extortion Trends*, available at https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends

contained within.[29] In 2020, over 50% of ransomware attackers exfiltrated data from a network before encrypting it.[30] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[31] And even where companies pay for the return of data attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[32]

61. 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."[33]

62. Defendant has not publicly shared many details of the Data Breach. However, based on Defendant's limited statements, third party reports from reputable sources, and Quantum's *modus operandi*, it is clear Defendant did not take reasonable precautions that would have allowed it to quickly detect, prevent, stop, undo, or remediate the effects of the Data Breach. These failures allowed cybercriminals using well publicized attack practices to access and steal the Private Information Defendant maintained on millions of individuals.

63. It is more likely than not that one or more PFC employees interacted with a Quantum phishing email, allowing Quantum to deploy IcedID malware on PFC's network.[34]

64. The FBI and Treasury Department published a Joint Cybersecurity Advisory in September 2021 warning companies like PFC that Conti, which partially merged into Quantum a

[29] *The chance of data being stolen in a ransomware attack is greater than one in ten*, available at https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/

[30] 2020 Ransomware Marketplace Report, available at https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report

[31] *Id.*

[32] *Id.*

[33] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Aug. 23, 2021).

[34] https://www.cybereason.com/blog/cybereason-vs.-quantum-locker-ransomware (last visited Oct. 25, 2022).

few months after the Advisory, was known to initiate cyberattacks through phishing campaigns and the deployment of IcedID malware.[35]

65. It has been reported that Quantum was then able to move "laterally inside" PFC's network "using Cobalt Strike and exfiltrating data via command-line tools."[36]

66. The September 2021 Cybersecurity Advisory similarly warned companies that Conti threat actors were known to use Cobalt Strike.[37]

67. Widely available software, such as the AI-Driven Cybereason XDR Platform, is able to "fully detect[] and prevent[] the Quantum Locker."[38]

68. The AI-driven Cybereason XDR Platform is able to prevent the execution of the Quantum Locker using multi-layer protection that detects and blocks malware with threat intelligence, machine learning, and next-gen antivirus (NGAV) capabilities. Additionally, when the Anti-Ransomware feature is enabled, behavioral detection techniques in the platform are able to detect and prevent any attempt to encrypt files and generates a MalOp for it:

MalOp for Quantum Locker as shown in the Cybereason XDR Platform

69. Using the Anti-Malware feature, the Cybereason XDR Platform will also detect and prevent the execution of the ransomware and ensure that it cannot encrypt targeted files.

---

[35] https://www.cisa.gov/uscert/sites/default/files/publications/AA21-265A-Conti_Ransomware_TLP_WHITE.pdf (last visited Oct. 30, 2022).
[36] https://www.bleepingcomputer.com/news/security/quantum-ransomware-attack-affects-657-healthcare-orgs/ (last visited Oct. 25, 2022).
[37] https://www.cisa.gov/uscert/sites/default/files/publications/AA21-265A-Conti_Ransomware_TLP_WHITE.pdf (last visited Oct. 30, 2022).
[38] https://www.cybereason.com/blog/cybereason-vs.-quantum-locker-ransomware (last visited Oct. 25, 2022).

70. The following industry standard security measures are known to specifically mitigate the risk of a Quantum cyberattack:

a. Organizations should implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and severs in a separate, segmented, and secure location.

b. Organizations should implement network segmentation and have offline backups of data.

c. Back up data regularly and password protect backup copies offline. Copies of critical data should not be accessible for modification or deletion from the system where data resides.

d. Organizations should emphasize network investigation tools that are used for exfiltration-centric groups (Cobalt Strike, Metasploit, and customized PowerShell Commands.

e. Track abnormal signaling to assist in identifying beacons.

f. The BazarCall attack vector relies on the execution of a beacon or malicious payload into the network system, which is liable to spread to other devices on the network. Separating the device while mitigating the BazarCall breach minimizes the chance that the infection will be able to affect other devices.

g. To identify Cobalt Strike, examine the network traffic using TLS inspection, then isolate bot traffic and identify the suspicious traffic by examining data within HTTPS requests.

71. The following industry standard network-based security practices are known to be particularly effective against Quantum cyberattacks:

a. Use and maintain anti-virus software and a firewall.

b. Regularly scan for spyware.

c. Keep software up to date.

d. Evaluate your software settings.

e. Avoid unused software programs.

f. Establish guidelines for computer use.

g. Encrypt sensitive files.

h. Dispose of sensitive information properly.

i. The following industry standard physical security practices are known to be particularly effective against Quantum cyberattacks:

j. Password-protect all computers.

k. Consider using physical locks on devices with sensitive information.

l. Consider an alarm or lock.

m. Implement physical access control plans.

72. Before the Data Breach, Defendant knew or should have known that the above security measures were necessary for the prevention of a data breach of this nature.

73. Defendant also could have prevented the Data Breach by encrypting the systems and files containing the Private Information of Plaintiffs and Class Members and by destroying Private Information it no longer had a legitimate need for.

74. Additionally, to prevent and detect unauthorized cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures known to be generally effective at mitigating the risk of a cyberattack:

- 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 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.[39]

75. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (Oss) have been updated with the latest patches. Vulnerable applications and Oss are the target of most ransomware attacks. . . .

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net). . . .

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it. . . .

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find

[39] How to Protect Your Networks from RANSOMWARE, at 3-4, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Aug. 23, 2021).

> information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
>
> - **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic. . . .[40]

76. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

> **Secure internet-facing assets**
>
> - Apply latest security updates
> - Use threat and vulnerability management
> - Perform regular audit; remove privileged credentials;
>
> **Thoroughly investigate and remediate alerts**
>
> - Prioritize and treat commodity malware infections as potential full compromise;
>
> **Include IT Pros in security discussions**
>
> - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
>
> **Build credential hygiene**
>
> - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
>
> **Apply principle of least-privilege**
>
> - Monitor for adversarial activities
> - Hunt for brute force attempts
> - Monitor for cleanup of Event Logs
> - Analyze logon events

[40] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Aug. 23, 2021).

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].[41]

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

78. 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 unauthorized exposure and exfiltration of the Private Information of Plaintiffs and Class Members.

79. As evidenced by its computer systems in need of security upgrades, as well as inadequate procedures for handling email phishing attacks, viruses, malignant computer code, and hacking attacks, Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

80. Defendant's negligence in safeguarding the Private Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

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

[41] *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/ (last visited Aug. 23, 2021).

Value of Private Information

82. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[42] 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."[43]

83. The Private Information 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. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[44] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[45] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[46]

84. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[47] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data

[42] 17 C.F.R. § 248.201 (2013).
[43] *Id.*
[44] *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/ (last visited Oct. 27, 2021).
[45] *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/ (last visited Oct. 27, 2021).
[46] *In the Dark*, VPNOverview, 2019, *available at* https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 27, 2021).
[47] *Data Brokers*, Los Angeles Times, Nov. 5, 2019, *available at* https://www.latimes.com/business/story/2019-11-05/column-data-brokers

broker who in turn aggregates the information and provides it to marketers or app developers.4849 Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[50]

85. The integrity of Private Information gives it its value because Private Information is used to secure loans, open lines of credit, verify identities, and unlock government benefits. When Private Information is used to commit fraud, these simple everyday necessities become more difficult, if not impossible, due to lowered credit scores and tarnished credit histories from credit fraud and identity theft.[51]

86. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its acquisition by cybercriminals and is likely already available on the dark web due to its high value for threat actors. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss.

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

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, 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

---

[48] https://datacoup.com/

[49] https://digi.me/what-is-digime/

[50] *Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at* https://computermobilepanel.nielsen.com/ui/US/en/faqen.html

[51] https://lifelock.norton.com/learn/identity-theft-resources/lasting-effects-of-identity-theft

> payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[52]

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

89. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The 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."[53]

90. Based on the foregoing, the Private 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 number and name.

91. 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."[54]

---

[52] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Oct. 27, 2021).
[53] 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 (last visited Oct. 27, 2021).
[54] Time 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 (last visited Aug. 23, 2021).

92. 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.

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

94. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."

95. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase Private Information, and PHI in particular, on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

96. According to account monitoring company LogDog, medical data, such as PHI, sells for $50 and up on the Dark Web.[55]

97. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may

[55] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), *available at* https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last visited July 20, 2021).

> continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[56]

98. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, including Social Security numbers, 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 Plaintiffs and Class Members as a result of a breach.

99. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages, in addition to any fraudulent use of their Private Information.

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

101. To date, Defendant has offered Plaintiffs and Class Members only 12 months of single bureau credit monitoring services through Experian. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the Private Information at issue here. Moreover, Defendant put the burden squarely on Plaintiffs and Class Members to enroll in the inadequate monitoring services that it offered.

---

[56] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at* https://www.gao.gov/assets/gao-07-737.pdf (last visited Aug. 23, 2021).

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

103. As a condition of providing medical treatment and services, processing medical claims, sending bills, and providing collection services for treatment, Defendant requires that its customers entrust it with Private Information.

104. By obtaining, collecting, using, and deriving a benefit from Plaintiffs and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

105. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

106. Plaintiffs and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business and health care purposes, and to prevent the unauthorized disclosures of the Private Information.

Defendant's Conduct Violates HIPAA

107. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, et seq. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII and PHI like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

108. Defendant is a business associate of a covered entity pursuant to HIPAA. *See* 45 C.F.R. § 160.102. Defendant must therefore comply with the HIPAA Privacy Rule and Security Rule. *See* 45 C.F.R. Part 160 and Part 164, Subparts A through E.

109. Defendant is a business associate of a covered entity pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

110. Plaintiffs' and Class Members' Private Information is "protected health information" as defined by 45 CFR § 160.103.

111. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

112. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

113. Plaintiffs' and Class Members' Private Information is "unsecured protected health information" as defined by 45 CFR § 164.402.

114. Plaintiffs' and Class Members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

115. Plaintiffs' and Class Members' unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

116. Plaintiffs' and Class Members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a

result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

117. Plaintiffs' and Class Members' unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

118. After receiving notice that they were victims of a data breach that required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it is reasonable for recipients of that notice, including Plaintiffs and Class Members in this case, to believe that future harm (including identity theft) is real and imminent, and to take steps to mitigate that risk of future harm.

119. The Data Breach could have been prevented if Defendant implemented HIPAA mandated, industry standard policies and procedures for securely disposing of Private Information when it was no longer necessary and/or had honored its obligations to its patients.

120. It can be inferred from Defendant's Data Breach that Defendant either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Plaintiffs' and Class Members' Private Information.

Defendant Failed to Comply with FTC Guidelines

121. Defendant was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

122. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that 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.[57]

123. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[58] The 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.

124. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private 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.[59]

125. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting

---

[57] FEDERAL TRADE COMMISSION, *Start With Security: A Guide for Business*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited July 7, 2022).
[58] FEDERAL TRADE COMMISSION, *Protecting Personal Information: A Guide for Business*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited July 7, 2022).
[59] FTC, *Start With Security*, *supra*.

from these actions further clarify the measures businesses must take to meet their data security obligations.

126. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

127. Defendant was at all times fully aware of its obligation to protect the PII stored within its systems because of its position as a leading healthcare business affiliate. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Plaintiff Blake's Experiences

128. Plaintiff Blake is a former patient of Choctaw Regional Medical Center, a healthcare provider client of Defendant.

129. In early 2022, as a condition of receiving medical services, Plaintiff Blake provided his first and last name, address, Social Security number, and other Private Information directly to Choctaw Regional Medical Center and indirectly to Defendant with the expectation that his Private Information would remain confidential.

130. Plaintiff Blake entrusted that his Private Information would be safeguarded according to internal policies and state and federal law.

131. Upon information and belief, Plaintiff Blake's Private Information was stored on Defendant's network during the Data Breach and presently remains in Defendant's possession.

132. On approximately July 1, 2022, Defendant notified Plaintiff Blake that Defendant's network had been accessed by unauthorized third parties and that Plaintiff Blake's Private Information may have been involved in the Data Breach.

133. Plaintiff Blake is very careful about sharing his sensitive Private Information. Plaintiff Blake has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Blake stores any documents containing his Private Information in a safe and secure location or destroys the documents.

134. As a result of the Data Breach, Plaintiff Blake has spent time dealing with the consequences of the Data Breach, which include time spent verifying the legitimacy of the Notice of Data Security Incident, exploring credit monitoring and identity theft protection services, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Indeed, in the notice letter Plaintiff received, PFC directed Plaintiff to spend time mitigating his losses: "You should always remain vigilant and monitor your accounts for suspicious or unusual activity."

135. Plaintiff Blake suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that Plaintiff Blake entrusted to Defendant, which was compromised in and as a result of the Data Breach.

136. Plaintiff Blake also experienced actual injury in the form of fraudulent activity on his debit card. Specifically, in approximately May 2022, Plaintiff Blake was traveling when his debit card was declined by a retailer. Plaintiff Blake called his bank and learned that there had been an unauthorized charge on his debit card for approximately $733. As a result of this unauthorized charge, Plaintiff Blake's bank locked his checking account. Because Plaintiff was away from home and could not verify his identity to his bank in person, he was unable to access his checking account for approximately two weeks.

137. As a result of the fraudulent activity caused by the Data Breach, Plaintiff Blake experienced a complete loss of access to debit funds and was forced to borrow money from friends

until his bank unlocked his account. The lack of access to funds caused Plaintiff Blake to miss bill payments, resulting in late fees.

138. Additionally, since approximately April 2022, Plaintiff Blake has been receiving insurance claims from his prior insurance provider for old medical services he did not re-submit. Upon information and belief, these claims are being fraudulently re-submitted as a result of the Data Breach.

139. Plaintiff Blake has suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

140. Plaintiff Blake has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of unauthorized third parties and possibly criminals. This injury was worsened by Defendant's delay in revealing the true nature of the threat to Plaintiff's Private Information.

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

Plaintiff McGarrigle's Experiences

142. Plaintiff McGarrigle is a former patient of Santa Fe Radiology, a healthcare provider client of Defendant.

143. In approximately September 2019, as a condition of receiving medical services, Plaintiff McGarrigle provided his first and last name, address, sensitive medial information, and other Private Information directly to Santa Fe Radiology and indirectly to Defendant with the expectation that his Private Information would remain confidential.

144. Plaintiff McGarrigle entrusted that his Private Information would be safeguarded according to internal policies and state and federal law.

145. Upon information and belief, Plaintiff McGarrigle's Private Information was stored on Defendant's network during the Data Breach and presently remains in Defendant's possession.

146. On approximately July 1, 2022, Defendant notified Plaintiff McGarrigle that Defendant's network had been accessed by unauthorized third parties and that Plaintiff McGarrigle's Private Information may have been involved in the Data Breach.

147. Plaintiff McGarrigle is very careful about sharing his sensitive Private Information. Plaintiff McGarrigle has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff McGarrigle stores any documents containing his Private Information in a safe and secure location or destroys the documents.

148. As a result of the Data Breach, Plaintiff McGarrigle has spent time dealing with the consequences of the Data Breach, which include time spent verifying the legitimacy of the Notice of Data Security Incident, exploring credit monitoring and identity theft protection services, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Indeed, in the notice letter Plaintiff received, PFC directed Plaintiff to spend time mitigating his losses: "You should always remain vigilant and monitor your accounts for suspicious or unusual activity."

149. Plaintiff McGarrigle suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that Plaintiff McGarrigle entrusted to Defendant, which was compromised in and as a result of the Data Breach.

150. Plaintiff McGarrigle experienced actual injury in the form of fraudulent activity on both his credit and debit cards. Specifically, in approximately June 2022, Plaintiff McGarrigle had

three separate unauthorized charges on his debit card from Google in the amounts of $99.99. Plaintiff McGarrigle spent significant time working with his bank to resolve the unauthorized charges.

151. Additionally, since the Data Breach, Plaintiff McGarrigle experienced unauthorized activity on his credit card, resulting in the cancellation of that card. As a result of the cancellation of his credit card, Plaintiff McGarrigle was forced to borrow money from friends to meet his daily needs until he received a new card from his bank.

152. In August 2022, Plaintiff McGarrigle noticed a decrease in his credit score that he is unable to account for, in connection with an unfamiliar hit by a collections company. Upon information and belief, Plaintiff McGarrigle believes that this credit score decrease is a ramification of the Data Breach.

153. Plaintiff McGarrigle has also experienced a substantial increase in suspicious phone calls and emails since the Data Breach, which Plaintiff McGarrigle believes is related to his Private Information being placed in the hands of illicit actors.

154. Plaintiff McGarrigle suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

155. Plaintiff McGarrigle has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of unauthorized third parties and possibly criminals. This injury was worsened by Defendant's delay in revealing the true nature of the threat to Plaintiff's Private Information.

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

Plaintiff Rodriguez's Experiences

157. Plaintiff Rodriguez is a former patient of Radiology Limited, a healthcare provider client of Defendant.

158. Over the course of several years, as a condition of receiving medical services, Plaintiff Rodriguez provided her first and last name, address, Social Security number, sensitive medial information, and other Private Information directly to Radiology Limited and indirectly to Defendant with the expectation that her Private Information would remain confidential.

159. Plaintiff Rodriguez entrusted that her Private Information would be safeguarded according to internal policies and state and federal law.

160. Upon information and belief, Plaintiff Rodriguez's Private Information was stored on Defendant's network during the Data Breach and presently remains in Defendant's possession.

161. On approximately July 1, 2022, Defendant notified Plaintiff Rodriguez that Defendant's network had been accessed by unauthorized third parties and that Plaintiff Rodriguez's Private Information may have been involved in the Data Breach.

162. Plaintiff Rodriguez is very careful about sharing her sensitive Private Information. Plaintiff Rodriguez has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Rodriguez stores any documents containing her Private Information in a safe and secure location or destroys the documents.

163. As a result of the Data Breach, Plaintiff Rodriguez has spent time dealing with the consequences of the Data Breach, which include time spent verifying the legitimacy of the Notice

of Data Security Incident and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Indeed, in the notice letter Plaintiff received, PFC directed Plaintiff to spend time mitigating her losses: "You should always remain vigilant and monitor your accounts for suspicious or unusual activity."

164. Plaintiff Rodriguez suffered actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that Plaintiff Rodriguez entrusted to Defendant, which was compromised in and as a result of the Data Breach.

165. Plaintiff Rodriguez experienced actual injury from the Data Breach in the form of identity theft. Specifically, in approximately March 2022, Plaintiff Rodriguez was notified that a third party was using her Social Security number. Plaintiff Rodriguez was applying for state benefits through the Arizona Department of Economic Security when she learned that her Social Security number was associated with employment at a company that Plaintiff had never heard of prior to the application. Plaintiff wrote a letter to the benefits office explaining that she did not work for this unfamiliar company. This issue caused a delay in the approval of Plaintiff Rodriguez's state benefits.

166. Plaintiff Rodriguez has also experienced a substantial increase in suspicious phone calls and text messages since the Data Breach, which Plaintiff Rodriguez believes is related to her Private Information being placed in the hands of illicit actors. Many of these suspicious phone calls and text messages are solicitations from medical companies for medical equipment and devices.

167. Plaintiff Rodriguez suffered lost time, annoyance, interference, and inconvenience

because of the Data Breach and has anxiety and increased concerns for the loss of her privacy. Plaintiff Rodriguez now checks her credit every day, with the concern that someone is continuing to use her Private Information to cause her harm.

168. Plaintiff Rodriguez has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of unauthorized third parties and possibly criminals. This injury was worsened by Defendant's delay in revealing the true nature of the threat to Plaintiff's Private Information.

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

Plaintiff Schroeder's Experience

170. Plaintiff Schroeder is a patient of Renown Regional Medical Center, a healthcare provider client of Defendant.

171. Over the course of several years, as a condition of receiving medical services, Plaintiff Schroeder provided his first and last name, address, Social Security number, sensitive medial information, and other Private Information directly to Renown Regional Medical Center and indirectly to Defendant with the expectation that his Private Information would remain confidential.

172. Plaintiff Schroeder entrusted that his Private Information would be safeguarded according to internal policies and state and federal law.

173. Upon information and belief, Plaintiff Schroeder's Private Information was stored on Defendant's network during the Data Breach and presently remains in Defendant's possession.

174. On or around July 10, 2022, Plaintiff Schroeder received notice from Defendant that its network had been accessed by unauthorized third parties and that Plaintiff Schroeder's Private Information may have been involved in the Data Breach.

175. Plaintiff Schroeder is very careful about sharing his sensitive Private Information. Plaintiff Schroeder has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Schroeder stores any documents containing his Private Information in a safe and secure location or destroys the documents.

176. As a result of the Data Breach, Plaintiff Schroeder has spent time dealing with the consequences of the Data Breach, which include time spent verifying the legitimacy of the Notice of Data Security Incident and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Indeed, in the notice letter Plaintiff received, PFC directed Plaintiff to spend time mitigating his losses: "You should always remain vigilant and monitor your accounts for suspicious or unusual activity."

177. Plaintiff Schroeder suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that Plaintiff Schroeder entrusted to Defendant, which was compromised in and as a result of the Data Breach.

178. Plaintiff Schroeder suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and has anxiety and increased concerns for the confirmed loss of his privacy, as well as the potential loss of his family members' privacy as a result of the Data Breach. As a military veteran, Plaintiff Schroeder is also especially concerned that cybercriminals may now have access to his retired pay, VA disability pay, military records, and benefits.

179. Plaintiff Schroeder has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of unauthorized third parties and possibly criminals. This injury was worsened by Defendant's delay in revealing the true nature of the threat to Plaintiff's Private Information.

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

Plaintiff Skrabo's Experience

181. Plaintiff Skrabo is a former patient of Dr. Andy Fine Primary Healthcare, a healthcare provider client of Defendant,

182. Over the course of several years, as a condition of receiving medical services, Plaintiff Skrabo provided his first and last name, address, sensitive medial information, and other Private Information directly to Dr. Andy Fine Primary Healthcare and indirectly to Defendant with the expectation that his Private Information would remain confidential.

183. Plaintiff Skrabo trusted that his Private Information would be safeguarded according to internal policies and state and federal law.

184. Upon information and belief, Plaintiff Skrabo's Private Information was stored on Defendant's network during the Data Breach and presently remains in Defendant's possession.

185. On approximately July 1, 2022, Defendant notified Plaintiff Skrabo that Defendant's network had been accessed by unauthorized third parties and that Plaintiff Skrabo's Private Information may have been involved in the Data Breach.

186. Plaintiff Skrabo is very careful about sharing his sensitive Private Information. Plaintiff Skrabo has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Skrabo stores any documents containing his Private Information in a safe and secure location or destroys the documents.

187. As a result of the Data Breach, Plaintiff Skrabo has spent time dealing with the consequences of the Data Breach, which include time spent verifying the legitimacy of the Notice of Data Security Incident, exploring credit monitoring and identity theft protection services, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Indeed, in the notice letter Plaintiff received, PFC directed Plaintiff to spend time mitigating his losses: "You should always remain vigilant and monitor your accounts for suspicious or unusual activity."

188. Plaintiff Skrabo suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that Plaintiff Skrabo entrusted to Defendant, which was compromised in and as a result of the Data Breach.

189. Plaintiff Skrabo experienced actual injury as a result of the Data Breach. Specifically, since the Data Breach, Plaintiff Skrabo has been notified several times that his Private Information was found on the Dark Web.

190. Additionally, since the Data Breach, Plaintiff Skrabo has experienced a substantial increase in suspicious phone calls and emails, which Plaintiff Skrabo believes is related to his Private Information being placed in the hands of illicit actors.

191. Plaintiff Skrabo suffered lost time, annoyance, interference, and inconvenience

because of the Data Breach and has anxiety and increased concerns for the loss of his privacy. Plaintiff Skrabo sent several hours resetting his account passwords and automatic billing information after learning of the Data Breach.

192. Plaintiff Skrabo has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of unauthorized third parties and possibly criminals. This injury was worsened by Defendant's delay in revealing the true nature of the threat to Plaintiff's Private Information.

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

Plaintiff Willingham's Experience

194. Plaintiff Willingham is a former patient of Touchstone Imaging, a business associate of Defendant.

195. In approximately 2019, as a condition of receiving medical services, Plaintiff Willingham provided her first and last name, address, sensitive medial information, and other Private Information directly to Touchstone Imaging and indirectly to Defendant with the expectation that her Private Information would remain confidential.

196. Plaintiff Willingham trusted that her Private Information would be safeguarded according to internal policies and state and federal law.

197. Upon information and belief, Plaintiff Willingham's Private Information was stored on Defendant's network during the Data Breach and presently remains in Defendant's possession.

198. On approximately July 1, 2022, Defendant notified Plaintiff Willingham that Defendant's network had been accessed by unauthorized third parties and that Plaintiff Willingham's Private Information may have been involved in the Data Breach.

199. Plaintiff Willingham is very careful about sharing her sensitive Private Information. Plaintiff Willingham has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Willingham stores any documents containing her Private Information in a safe and secure location or destroys the documents.

200. As a result of the Data Breach, Plaintiff Willingham has spent time dealing with the consequences of the Data Breach, which include time spent verifying the legitimacy of the Notice of Data Security Incident, exploring credit monitoring and identity theft protection services, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Indeed, in the notice letter Plaintiff received, PFC directed Plaintiff to spend time mitigating her losses: "You should always remain vigilant and monitor your accounts for suspicious or unusual activity."

201. Plaintiff Willingham suffered actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that Plaintiff Willingham entrusted to Defendant, which was compromised in and as a result of the Data Breach.

202. Plaintiff Willingham has also experienced a substantial increase in suspicious phone calls since the Data Breach, which Plaintiff Willingham believes is related to her Private Information being placed in the hands of illicit actors.

203. Plaintiff Willingham suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

204. Plaintiff Willingham has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of unauthorized third parties and possibly criminals. This injury was worsened by Defendant's delay in revealing the true nature of the threat to Plaintiff's Private Information.

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

CLASS ALLEGATIONS

206. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

207. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> **All United States residents whose Private Information was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Data Breach that Defendant published to Plaintiffs and other Class Members on or around July 1, 2022 (the "Nationwide Class").**

208. Plaintiff Rodriguez seeks to represent the following class of Arizona residents as follows:

> **All Arizona residents whose Private Information was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Data Breach that Defendant published to Plaintiffs and other Class Members on or around July 1, 2022 (the "Arizona Class").**

209. Plaintiff McGarrigle seeks to represent the following class of California residents as follows:

> **All California residents whose Private Information was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Data Breach that Defendant published to Plaintiffs and other Class Members on or around July 1, 2022 (the "California Class").**

210. Plaintiff Schroeder seeks to represent the following class of Nevada residents as follows:

> **All Nevada residents whose Private Information was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Data Breach that Defendant published to Plaintiff and other Class Members on or around July 1, 2022 (the "Nevada Class").**

211. Plaintiff Skrabo seeks to represent the following class of Colorado residents as follows:

> **All Colorado residents whose Private Information was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Data Breach that Defendant published to Plaintiff and other Class Members on or around July 1, 2022 (the "Colorado Class").**

212. 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; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

213. Plaintiffs reserve the right to modify or amend the definition of the proposed Classes before the Court determines whether certification is appropriate.

214. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds of thousands, if not millions, of individuals whose Private Information may have been improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant's records.

215. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;

b. Whether Defendant had duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the Private Information of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiffs and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information 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 that permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members;

k. Whether Defendant violated the consumer protection statutes invoked herein;

l. Whether Plaintiffs and Class Members are entitled to actual, incidental, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

m. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

n. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

216. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach due to Defendant's misfeasance.

217. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has 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 Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to an individual Plaintiff.

218. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class, and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

219. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): 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.

220. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs 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 Plaintiffs were 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.

221. 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.

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

223. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information 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.

224. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

225. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

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

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

g. 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;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members;

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

226. Plaintiffs repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

227. Plaintiffs and the Class entrusted Defendant with their Private Information.

228. The Private Information of Plaintiffs and the Class was entrusted to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their Private Information for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

229. Defendant has and had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

230. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiffs and the Class involved an unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the criminal acts of a third party.

231. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the Private Information of Plaintiffs and the Class in Defendant's possession was adequately secured and protected.

232. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information it was no longer required to retain pursuant to regulations.

233. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the Private Information of Plaintiffs and the Class.

234. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Private Information, a necessary part of obtaining services from Defendant. That duty further arose because Defendant chose to collect and maintain the Private Information for its own pecuniary benefit.

235. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Class.

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

237. Plaintiffs and the Class's injuries were the foreseeable and probable result of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

238. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the Class. Defendant's misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included

their decisions not to comply with industry standards for the safekeeping of the Private Information of Plaintiffs and the Class, including basic encryption techniques freely available to Defendant.

239. Plaintiffs and the Class had no ability to protect their Private Information that was within, and on information and belief remains within, Defendant's possession.

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

241. Defendant had (and continues to have) a duty to adequately disclose that the Private Information of Plaintiffs 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 Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

242. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the Private Information of Plaintiffs sand the Class.

243. Defendant has admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

244. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Private Information of Plaintiffs and the Class during the time the Private Information was within Defendant's possession or control.

245. Defendant improperly and inadequately safeguarded the Private Information of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

246. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the Private Information of Plaintiffs and the Class in the face of increased risk of theft.

247. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of Private Information.

248. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Nationwide Class, the Private Information of Plaintiffs and the Class would not have been compromised.

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

250. Additionally, Section 5 of the FTC Act 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 Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

251. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and by not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and

amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

252. Defendant's violation of Section 5 of the FTC Act is, in and of itself, evidence of Defendant's negligent data security practices and further constitutes negligence *per se*.

253. Plaintiffs and the Class are within the class of persons that the FTC Act was intended to protect.

254. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. 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 Plaintiffs and the Class.

255. Defendant is a business associate of a covered entity pursuant to HIPAA. *See* 45 C.F.R. § 160.102. Defendant must therefore comply with the HIPAA Privacy Rule and Security Rule. See 45 C.F.R. Part 160 and Part 164, Subparts A through E.

256. Plaintiffs' and Class Members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

257. Defendant's violations of 45 CFR Subpart E are, in and of themselves, evidence of Defendant's negligence and further constitute negligence *per se.*

258. Plaintiffs and Class Members are within the class of persons that HIPAA was intended to protect.

259. The harm that occurred as a result of the Data Breach is the type of harm HIPAA was intended to guard against.

260. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to decide how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of Plaintiffs and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class.

261. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

262. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendant's possession and is subject to

further unauthorized disclosures so long as Defendant continues to fail to undertake appropriate and adequate data security measures to protect the Private Information in its continued possession.

263. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class)

264. Plaintiffs repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

265. The Private Information of Plaintiffs and the Class, including, without limitation, first and last name, address, accounts receivable balance and information regarding payments made to accounts, and, in some cases, date of birth, Social Security numbers, and health insurance and medical treatment information, was provided and entrusted to Defendant.

266. Plaintiffs and the Class provided their Private Information to Defendant, either directly or indirectly through Defendant's clients, as part of Defendant's regular business practices.

267. As a condition of obtaining care and/or services from Defendant's clients, Plaintiffs and the Class provided and entrusted their Private Information. In so doing, Plaintiffs 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 Plaintiffs and the Class if their data had been breached and compromised or stolen.

268. A meeting of the minds occurred when Plaintiffs and the Class agreed to, and did, provide their Private Information to Defendant and/or Defendant's clients with the reasonable understanding that their Private Information would be adequately protected by any business associates, like Defendant, from foreseeable threats. This inherent understanding exists

independent of any other law or contractual obligation any time that highly sensitive PII and PHI is exchanged as a condition of receiving services. It is common sense that but for this implicit and/or explicit agreement, Plaintiffs and Class Members would not have provided their Private Information.

269. Defendant separately has contractual obligations arising from and/or supported by the consumer facing statements in its Privacy Policies.

270. Defendant also has contractual obligations arising out of its status as a business associate of covered entities pursuant to HIPAA. These contracts included, in part, promises regarding Defendant's commitment to the security of patient privacy.

271. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

272. Defendant breached the implied contracts it made with Plaintiffs and the Class by failing to safeguard and protect their Private Information and by failing to provide timely and accurate notice that Private Information was compromised as a result of the Data Breach.

273. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

274. As a result of Defendant's breach of implied contract, Plaintiffs and the Class are entitled to and demand actual, consequential, and nominal damages.

COUNT III
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiff and the Nationwide Class)

275. Plaintiffs repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

276. Plaintiffs bring this claim for breach of third-party beneficiary contract against PFC in the alternative to Plaintiffs' claim for breach of implied contract.

277. PFC entered into various contract with its healthcare provider clients to provide accounts receivable management services to its clients.

278. These contracts are virtually identical to each other and were made expressly for the benefit of Plaintiffs and the Class, as it was their confidential medical information that PFC agreed to collect and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties.

279. PFC knew that if it were to breach these contracts with its healthcare provider clients, the clients' patients, including Plaintiffs and the Class, would be harmed by, among other things, fraudulent misuse of their Private Information.

280. PFC breached its contracts with its clients when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiffs' and Class Members' Private Information.

281. As reasonably foreseeable, Plaintiffs and the Class were harmed by PFC's failure to use reasonable data security measures to store their Private Information, including but not limited to, the actual harm through the loss of their Private Information to cybercriminals.

282. Accordingly, Plaintiffs and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action

COUNT IV
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Nationwide Class)

283. Plaintiffs repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

284. Plaintiffs and Class Members conferred a monetary benefit on Defendant by providing Defendant, directly or indirectly, with their valuable Private Information.

285. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information.

286. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

287. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiffs and Class Members because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

288. Defendant acquired the monetary benefit and Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

289. If Plaintiffs and Class Members knew that Defendant had not secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

290. Plaintiffs and Class Members have no adequate remedy at law.

291. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

292. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

293. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them.

COUNT V
INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Nationwide Class)

294. Plaintiffs repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

295. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

296. Defendant owed a duty to Plaintiffs and Class Members to keep their Private Information confidential.

297. Defendant affirmatively disclosed Private Information through its interaction with and/or response to Quantum's phishing campaign.

298. The unauthorized disclosure of Plaintiffs' and Class Members' Private Information to an unauthorized third party is highly offensive to a reasonable person.

299. Defendant's reckless and negligent failure to protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure constitutes an intentional interference with Plaintiffs' and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

300. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

301. Defendant knowingly did not notify Plaintiffs and Class Members in a timely fashion about the Data Breach.

302. Because Defendant failed to properly safeguard Plaintiffs' and Class Members' Private Information, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

303. As a proximate result of Defendant's acts and omissions, the private and sensitive Private Information of Plaintiffs and Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

304. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their Private Information is still maintained by Defendant with its inadequate cybersecurity system and policies.

305. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's refusal to safeguard the Private Information of Plaintiffs and the Class.

306. Plaintiffs, on behalf of themselves and Class Members, seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs' and Class Members' Private Information.

307. Plaintiffs, on behalf of themselves and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant and the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT VI
VIOLATION OF COLORADO CONSUMER PROTECTION ACT
Colo. Rev. Stat. § 6-1-101, *et seq*.
(On behalf of Plaintiffs and the Nationwide Class, or alternatively, Plaintiff Skrabo and the Colorado Class)

308. Plaintiffs repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

309. The Colorado Consumer Protection Act ("Colorado CPA"), Colo. Rev. Stat. § 6-1-105(1)(l), *et seq*., prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service.

310. Defendant is a "person" under § 6-1-102(6) of the Colorado CPA, Colo. Rev. Stat. § 6-1-101, *et seq*.

311. Plaintiffs and the Class provided and/or entrusted sensitive and confidential PII and/or PHI to Defendant, which Defendant collected, stored, and maintained at its Colorado headquarters.

312. Defendant is engaged in, and its acts and omissions affect, trade and commerce. Defendant's relevant acts, practices, and omissions complained of in this action were done in the course of Defendant's business of marketing, offering for sale, and selling goods and services throughout the United States.

313. In the conduct of its business, trade, and commerce, Defendant engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the provision or sale of services to consumers. Plaintiffs and other members of the Class furnished or purchased these services. Plaintiffs and the Class are actual or potential consumers as defined by Colo. Rev. Stat § 6-1-113(1), *et seq.*

314. In the conduct of its business, trade, and commerce, Defendant collected and stored highly personal and private information, including Private Information belonging to Plaintiffs and the Class.

315. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Private Information of Plaintiffs and the Nationwide Class and that the risk of a data breach was highly likely and/or that the risk of the data breach being more extensive than originally disclosed was highly likely.

316. Defendant should have disclosed this information regarding its computer systems and data security practices because Defendant was in a superior position to know the true facts related to its security practices, and Plaintiffs and the Class could not reasonably be expected to learn or discover the true facts.

317. As alleged herein this Complaint, Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and the furnishing of customer relation services to consumers in violation of the Colorado CPA, including but not limited to the following:

a. failing to adequately secure consumer's names and Social Security numbers;

b. failing to maintain adequate computer systems and data security practices to safeguard consumers' Private Information;

c. failing to disclose the material information, known at the time of the transaction—collection and retention of consumer Private Information to furnish customer relation services—that its computer systems would not adequately protect and safeguard consumer Private Information;

d. inducing consumers to use Defendant's services by failing to disclose, and misrepresenting the material fact that, Defendant's computer systems and data security practices were inadequate to safeguard employee's and client's sensitive personal information from theft.

318. By engaging in the conduct delineated above, Defendant has violated the Colorado CPA by, among other things:

a. omitting material facts regarding the goods and services sold;

b. omitting material facts regarding the security of the transactions between Defendant and consumers;

c. omitting material facts regarding the security of the transactions between Defendant and consumers who furnished or entrusted their Personal Information;

d. misrepresenting material facts in the furnishing or sale of products, goods, or services to consumers;

e. engaging in conduct that is likely to mislead consumers acting reasonably under the circumstances;

f. engaging in conduct that creates a likelihood of confusion or of misunderstanding;

g. engaging in conduct with the intent to induce consumers to use Defendant's service;

h. unfair practices that caused or were likely to cause substantial injury to consumers that is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers; and/or

i. other unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices to be shown at trial.

319. Defendant systemically engaged in these deceptive, misleading, and unlawful acts and practices, to the detriment of Plaintiffs and the Class.

320. Defendant's actions in engaging in the conduct delineated above were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and Class.

321. As a direct result of Defendant's violation of the Colorado CPA, Plaintiffs and the Class have suffered actual damages, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect that Private Information; and (viii) present and future costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class.

322. As a result of Defendant's violation of the Colorado CPA, Plaintiffs and the Class are entitled to, and seek, injunctive relief, including, but not limited to:

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

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

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

d. Ordering that Defendant segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems are compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner employee and customer data not necessary for its provision of services;

f. Ordering that Defendant conduct regular database scanning and securing checks;

g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and,

h. Ordering Defendant to meaningfully educate its employees and customers about the threats they face as a result of the loss of their financial and personal

information to third parties, as well as the steps customers must take to protect themselves.

323. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices of Defendant alleged herein, Plaintiffs and putative Class Members seek relief under Colo. Rev. Stat. § 6-1-113, including, but not limited to, the greater of actual damages, statutory damages, or treble damages for bad faith conduct, injunctive relief, attorneys' fees and costs, as allowable by law.

COUNT VII
VIOLATION OF ARIZONA CONSUMER FRAUD ACT
Ariz. Rev. Stat. § 44-1521, *et seq*.
(On Behalf of Plaintiff Rodriguez and the Arizona Class)

324. Plaintiff Rodriguez and the Arizona Class re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

325. Defendant sold Plaintiff Rodriguez and the Arizona Class "merchandise" as that term as defined by A.R.S. § 44-1521, in the form of customer care services.

326. Section 44-1522 of the Arizona Consumer Fraud Act provides:

> The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby.
>
> *See* A.R.S. § 44-1522(A).

327. Defendant used deception, used a deceptive act or practice, and fraudulently omitted and concealed material facts in connection with the sale or advertisement of that merchandise in violation of A.R.S. §44-1522(A)

328. Defendant omitted and concealed material facts, which it knew about and had the duty to disclose—namely, Defendant's inadequate privacy and security protections for Plaintiff Rodriguez's and the Arizona Class's Private Information. Defendant omitted and concealed those material facts even though Defendant should have disclosed them in good conscience, and it did so with the intent that others would rely on the omission, suppression, and concealment.

329. The concealed facts are material in that they are logically related to the transactions at issue and rationally significant to the parties in view of the nature and circumstances of those transactions.

330. Plaintiffs do not allege any claims based on any affirmative misrepresentations by Defendant; rather Plaintiffs allege that Defendant omitted, failed to disclose and concealed material facts and information as alleged herein, despite its duty to do so.

331. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff Rodriguez's and the Arizona Class's Private Information, and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in these deceptive acts and practices were negligent, knowing, and willful, and wanton and reckless with respect to the rights of Plaintiff Rodriguez and the Arizona Class.

332. Plaintiffs and the Arizona Class were ignorant of the truth and the concealed facts and incurred damages as a consequent and proximate result.

333. Plaintiffs and the Arizona Class seek all available relief under A.R.S. § 44-1521, *et. seq*., including, but not limited to, compensatory damages, punitive damages, injunctive relief, and attorneys' fees and costs.

COUNT VIII
CALIFORNIA CUSTOMER RECORDS ACT
Cal. Civ. Code §§ 1798.80, *et seq.*
(On Behalf of Plaintiff McGarrigle and the California Class)

334. Plaintiff McGarrigle, individually and on behalf of the California Class, repeats and realleges the allegations contained in the preceding paragraphs of the Complaint as if fully set forth herein.

335. "To ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any 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."

336. Defendant is a business that owns, maintains, and licenses Personal Information ("PII"), within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiff McGarrigle and the California Class.

337. Businesses that own or license computerized data that includes PII, including Social Security numbers, medical information, and health information, are required to notify California residents when their PII has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

338. Defendant is a business that owns or licenses computerized data that includes PII as defined by Cal. Civ. Code § 1798.82.

339. Plaintiff McGarrigle and California Class Members' Private Information includes PII as covered by Cal. Civ. Code § 1798.82.

340. Because Defendant reasonably believed that Plaintiff's and California Class Members' PII was acquired by unauthorized persons during the Data Breach, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

341. Defendant failed to fully disclose material information about the Data Breach.

342. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated Cal. Civ. Code § 1798.82.

343. As a direct and proximate result of Defendant's violations of Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and California Class Members suffered damages as described above.

344. Plaintiffs and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT IX
VIOLATION OF CALIFORNIA's UNFAIR COMPETITION LAW
Cal. Bus. Code § 17200, *et seq.*
(On Behalf of Plaintiffs and the Class,
or on Behalf of Plaintiff McGarrigle and the California Class)

345. Plaintiffs and the Class reallege, as if fully set forth, the allegations of the proceeding paragraphs of the Complaint.

346. Defendant engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, et seq. which prohibits unlawful, unfair, or fraudulent business acts or practices ("UCL").

347. Defendant's conduct is unlawful because it violates the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, et seq. (the "CCPA"), and other state data security laws.

348. Defendant stored the Private Information of Plaintiffs and the Class in its computer systems and knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with applicable regulations and that would have kept Plaintiffs' and the Class's Private Information secure and prevented the loss or misuse of that PII.

349. Defendant failed to disclose to Plaintiffs and the Class that their Private Information was not secure. However, Plaintiffs and the Class were entitled to assume, and did assume, that Defendant had secured their Private Information. At no time were Plaintiffs and the Class on notice that their PII was not secure, which Defendant had a duty to disclose.

350. Defendant also violated California Civil Code § 1798.150 by failing to employ reasonable security measures, resulting in an unauthorized access and exfiltration, theft, or disclosure of Plaintiffs' and the Class's Private Information.

351. Had Defendant complied with these requirements, Plaintiffs and the Class would not have suffered the damages related to the data breach.

352. Defendant's conduct was unlawful, in that it violated the Consumer Records Act.

353. Defendant's conduct was also unfair, in that it violated a clear legislative policy in favor of protecting consumers from data breaches.

354. Defendant's conduct is an unfair business practice under the UCL because it was immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct includes employing unreasonable and inadequate data security despite its business model of actively collecting PII.

355. Defendant also engaged in unfair business practices under the "tethering test." Its actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

356. Instead, Defendant made the Private Information of Plaintiffs and the Class accessible to scammers, identity thieves, and other malicious actors, subjecting Plaintiffs and the Class to an impending risk of identity theft. Additionally, Defendant's conduct was unfair under the UCL because it violated the policies underlying the laws set out in the prior paragraph.

357. As a result of those unlawful and unfair business practices, Plaintiffs and the Class suffered an injury-in-fact and have lost money or property.

358. The injuries to Plaintiffs and the Class greatly outweigh any alleged countervailing benefit to consumers or competition under all of the circumstances.

359. There were reasonably available alternatives to further Defendant's legitimate business interests, other than the misconduct alleged in this complaint.

360. Therefore, Plaintiffs and the Class are entitled to equitable relief, including restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to Defendant because of its unfair and improper business practices; a permanent injunction enjoining

Defendant's unlawful and unfair business activities; and any other equitable relief the Court deems proper.

COUNT X
VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT ("CCPA")
Cal. Civ. Code 1798.150
(On Behalf of Plaintiff McGarrigle and the California Class)

361. Plaintiff McGarrigle and the California Class reallege, as if fully set forth, the allegations of the proceeding paragraphs of the Complaint.

362. Defendant violated § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted Private Information of Plaintiffs and the California Subclass. As a direct and proximate result, Plaintiff McGarrigle and the California Subclass's PII was subject to unauthorized access and exfiltration, theft, or disclosure.

363. Defendant is a business organized for the profit and financial benefit of its owners according to California Civil Code § 1798.140, that collects the personal information of its employees and whose annual gross revenues exceed the threshold established by California Civil Code § 1798.140(d).

364. Plaintiff McGarrigle and California Subclass members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold Private Information, including Plaintiff McGarrigle's and California Subclass members' Private Information. Plaintiff McGarrigle and California Subclass members have an interest in ensuring that their PII is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

365. Pursuant to California Civil Code § 1798.150(b), Plaintiff McGarrigle mailed a CCPA notice letter to Defendant's registered service agents, detailing the specific provisions of the CCPA that Defendant has violated and continues to violate. If Defendant cannot cure within 30 days—and Plaintiff Cruz believes such cure is not possible under these facts and circumstances—then Plaintiff Cruz intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

366. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information so as to protect the personal information under the CCPA.

367. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant.

COUNT XI
VIOLATION OF NEVADA CONSUMER FRAUD ACT
(On Behalf of Plaintiff Schroeder and the Nevada Class)

368. Plaintiff Schroeder and the Nevada Class reallege, as if fully set forth, the allegations of the proceeding paragraphs of the Complaint.

369. In the course of its business operations in Nevada, Defendant engaged in deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to its employment and/or business affiliation with persons in the State of Nevada in violation of Nev. Rev. Stat. § 598.0915. Defendant also violated Nev. Rev. Stat. § 598.0923(1)(c) because it violated state and federal laws in connection with the sale or lease of goods or services (i.e., the accounts receivable services it provided). Defendant's misrepresentations included but are not limited to the following:

a. Defendant misrepresented material facts pertaining to the storing of Plaintiffs' and the Nevada Class's Private Information by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Nevada Class Members' Private Information from unauthorized disclosure, release, data breaches, and theft, in violation of Nev. Rev. Stat. § 598.0915(15);

b. Defendant misrepresented material facts pertaining to the storage of the Private Information belonging to the Nevada Class by representing by implication that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Nevada Class Members' Private Information, in violation of Nev. Rev. Stat. § 598.0915(15);

c. Defendant omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Nevada Subclass Members' Private Information in violation of Nev. Rev. Stat. § 598.0915(15);

d. Defendant engaged in deceptive trade practices with respect to its employment of, and/or business affiliation with, Nevada Class Members and the Private Information of those Nevada Class Members, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including 15 U.S.C. § 45 and Nev. Rev. Stat. § 603A.210;

e. Defendant engaged in deceptive trade practices by failing to disclose the Data Breach to Nevada Class Members in a timely and accurate manner in their July communications and thereafter, in violation of Nev. Rev. Stat. § 603A.220(1);

f. Defendant engaged in deceptive trade practices by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Nevada Class Members' Private Information from further unauthorized disclosure, release, data breaches, and theft; and

g. Defendant violated Nev. Rev. Stat. § 598.0923(1)(c) because its violations of the FTC Act, HIPAA, Nev. Rev. Stat. § 603A, and Nev. Rev. Stat. § 598.0915(15) constituted a violation of a state or federal law.

370. The above unlawful deceptive acts and practices by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and the Nevada Class, which injury they could not reasonably avoid; this substantial injury outweighed any benefits to patients or to competition.

371. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Nevada Class Members' Private Information and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-described unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Nevada Class.

372. As a direct and proximate result of Defendant's deceptive practices, Nevada Class members suffered injury and/or damages.

373. Under Nev. Rev. Stat. § 41.600, violation of either Nev. Rev. Stat. § 598.0915 or Nev. Rev. Stat. § 598.0923(1)(c) constitutes actionable "consumer fraud."

374. Plaintiff and Nevada Class Members seek relief under Nev. Rev. Stat. Ann. § 41.600, including, but not limited to, injunctive relief, other equitable relief, actual damages, and attorneys' fees and costs.

375. Plaintiff and the Nevada Class Members also seek a declaration that Defendant's existing security measures do not comply with its obligations under the FTC Act, HIPAA, Nev. Rev. Stat. § 603A, and any other applicable federal or state law. Plaintiff seeks to enforce this declaratory relief through an affirmative injunction which requires the following:

a. Ordering that Defendant engage 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;

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

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

d. Ordering that Defendant segment the highly sensitive Personal Information by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

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

f. Ordering that Defendant conduct regular database scanning and securing checks;

g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Defendant to meaningfully educate its customers about the threats they face as a result of the loss of their patients' Private Information to third parties, as well as the steps Defendant's customers and the patients and current and former employees impacted by the Data Breach must take to protect themselves.

COUNT XII
DECLARATORY RELIEF
(On Behalf of Plaintiffs and the Nationwide Class)

376. Plaintiffs fully incorporate by reference all of the above paragraphs in the Complaint, as though fully set forth herein.

377. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

378. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiffs and Class Members' Private Information, as well as whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from future data breaches that compromise their Private Information. Plaintiffs and the Nationwide Class remain at imminent risk that further compromises of their Private Information will occur in the future.

379. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect employee and patient Private Information.

380. Defendant still possesses the Private Information of Plaintiffs and the Class.

381. To Plaintiffs' knowledge, Defendant has made no announcement that it has changed its data storage or security practices relating to the Private Information.

382. To Plaintiffs' knowledge, Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

383. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at PFC. The risk of another such breach is real, immediate, and substantial.

384. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at PFC, Plaintiffs and Class Members will likely continue to be subjected to fraud, identify 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.

385. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at PFC, thus eliminating the additional injuries that would result to Plaintiffs and Class Members, along with other patients and/or current and former PFC employees whose Private Information would be further compromised.

386. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Defendant implement and maintain reasonable security measures, including but not limited to the following:

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

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. purging, deleting, and destroying Private Information not necessary for its provisions of services in a reasonably secure manner;

e. conducting regular database scans and security checks; and

f. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Classes, and appointing Plaintiffs and their 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 Private Information of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs 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 their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the Private Information of Plaintiffs 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 Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;

vi. 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;

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

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

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

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

xi. 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 Plaintiffs and Class Members;

xii. 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;

xiii. 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;

xiv. 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;

xv. 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 themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and 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, but not limited to, actual, consequential, and nominal 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.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: November 3, 2022

Respectfully Submitted,

Jean S. Martin
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jeanmartin@ForThePeople.com

Terence R. Coates
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Telephone: 513.651.3700
Facsimile: 513.665.0219
tcoates@msdlegal.com

Joseph M. Lyon (OH BAR #76050)*
THE LYON LAW FIRM, LLC
2754 Erie Ave.
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com

Interim Co-Lead Counsel for Plaintiffs and Putative Class

CERTIFICATE OF SERVICE

I, Jean S. Martin, hereby certify that on November 3, 2022, a true and correct copy of PLAINTIFFS' CONSOLIDATED CLASS ACTION COMPLAINT was filed with the Court using its CM/ECF System which will alert all registered users of the filing.

/s/ Jean S. Martin
Jean S. Martin

ClassAction.org
