UNITED STATES DISTRICT COURT
DISTRICT OF COLORADO

MARKO SKRABO Individually and on Behalf of All Others Similarly Situated, Plaintiff, v. **PROFESSIONAL FINANCE COMPANY, INC.,** Defendant	**CASE NO.** **COMPLAINT- CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiff Marko Skrabo brings this action on behalf of himself, and all others similarly situated against Defendant, Professional Finance Company, Inc. ("PFC" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities, and alleges as follows:

INTRODUCTION

1. PFC, a Colorado-based accounts receivable management company, lost control of thousands of individuals' highly sensitive personal information in a data breach by cybercriminals discovered by PFC in February 2022 ("Data Breach"). On information and belief, sometime prior to February 26, 2022, cybercriminals were able to access and pilfer Mr. Skrabo's and Class members' information, including, but not limited to, first and last names, addresses, accounts receivable balances and information regarding payments made to accounts, and Social Security numbers (collectively, "PII") and, for some individuals, birth dates, Social Security numbers, and personal health information ("PHI") including health insurance information, and medical

treatment information (collectively "Private Information").

2. The Data Breach occurred because PFC fails to maintain adequate cyber security systems, fails to delete unneeded data with sensitive personal information, and fails to train its employees on reasonable security measures, leaving the information an unguarded target for theft and misuse. Mr. Skrabo has no affiliation with PFC and, as far as he knows, never provided his information to any of PFC's clients, but received notice from PFC that he was a victim of the Data Breach. He is asserting claims on behalf of himself, and all others harmed by PFC's misconduct.

3. According to its website, PFC "is an accounts receivable management company located in Greeley, Colorado. Thousands of national clients rely on [Defendant] to recover their receivables and manage their early out self-pay programs."[1] It purports to be one of the nation's leading debt recovery agencies, and its client list includes many healthcare providers, retailers, financial organizations, and government agencies.[2]

4. As a debt recovery agency, PFC necessarily receives vast amounts of Private Information from its clients' customers and patients and is charged with managing and protecting that Private Information. Its Privacy Policy states:[3]

[1] https://www.pfcusa.com/about-us/ (last visited July 23, 2022).
[2] https://www.hipaajournal.com/657-healthcare-providers-affected-by-ransomware-attack-on-professional-finance-company/ (last visited July 23, 2022).
[3] https://www.pfcusa.com/privacy-policy/ (last visited July 23, 2022).

Personal Information We Collect

Personal identification information is data that can be used to identify or contact you.

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 (URL) information (showing where you came from or where you go to next), email open rates, credit card, bank account information.

5. PFC's privacy policy also states that it "is serious about data security" and that it "seek[s] to implement the best practices in data collection, storage, processing, and security to protect against unauthorized access and disclosure."[4]

6. Despite those assurances, on February 26, 2022, PFC identified a cyber incident in which an unauthorized third party accessed and disabled some of its computer systems. PFC engaged a third-party forensic specialist and determined that 657 of its healthcare provider clients were affected. A list of all affected entities is attached as Exhibit 1.

7. PFC reviewed the data that was obtained in the Data Breach and Defendant confirmed that the data contained names, addresses, accounts receivable balances, information regarding payments made to accounts, and, for some individuals, birth dates, Social Security numbers, and personal health information including health insurance information, and medical treatment information.

[4] *Id.*

8. Despite learning of the Data Breach in February 2022, PFC did not begin notifying Plaintiff and Class Members until at least May 5, 2022, and in fact, Plaintiff's notice was dated July 1, 2022. Defendant delayed in sending notice of the Data Breach even though it is well 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.

9. As a result of the Data Breach, Plaintiff and likely millions of Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack and the substantial and imminent risk of identity theft.

10. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant admits that the unencrypted Private Information impacted during the Data Breach included names, addresses, dates of birth, Social Security numbers, diagnostic information, and health insurance information.

11. The exposed Private Information of Plaintiff and Class Members can—and likely will—be sold on the dark web. Hackers can offer for sale the unencrypted, unredacted Private Information to criminals. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

12. This Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the Private Information of Plaintiff and Class Members. In addition to Defendant's failure to prevent the Data Breach, after discovering the

breach, Defendant waited several months to report it to government agencies and affected individuals.

13. As a result of this delayed response, Plaintiff and Class Members had no idea their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

PARTIES

14. Plaintiff, Marko Skrabo, is a natural person and citizen of Colorado, where he intends to remain. Mr. Skrabo did not knowingly provide his Private Information to PFC, but received PFC's Breach Notice in July 2022 and subsequently called the telephone number established by PFC to confirm that he was a victim of the Data Breach.

15. 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 & VENUE

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

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

18. Venue is proper in this district because a substantial part of the events or omissions giving rise to the claim occurred in this District.

FACTUAL ALLEGATIONS

a. PFC

19. PFC is a Colorado-based debt recovery agency that serves thousands of clients in the healthcare, retail, finance, and governmental services industries.

20. As part of its business, PFC collects sensitive Private Information from its clients' customers in order to provide its services. The information collected includes, at least, "full name, date of birth, social security number, phone number, address, email address, account number, original creditor, current creditor, balance, payment history," promising to safeguard that data from theft and misuse using reasonable security measures.[5]

21. In so doing, PFC recognizes its duty to safeguard Private Information through its own Privacy Policy, available to the public on its website at https://www.pfcusa.com/privacy-policy/ and attached hereto as **Exhibit 2**.

22. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand Defendant safeguard their Private Information. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties.

23. Despite these assurances, on information and belief, PFC has not implemented reasonable cybersecurity safeguards or policies to protect Private Information, or trained its

[5] *Id.*

employees to prevent, detect, and stop data breaches of PFC's systems. As a result, PFC leaves vulnerabilities for cybercriminals to exploit and give access to Private Information.

b. PFC Fails to Safeguard Private Information

24. PFC obtains troves of Private Information about Plaintiff and the Class not from Plaintiff and the Class themselves but from its clients.

25. PFC collects and maintains this Private Information in its computer systems.

26. In collecting and maintaining the Private Information, PFC agreed it would safeguard the data according to its internal policies and state and federal law.

27. Still, sometime prior to February 26, 2022, cybercriminals bypassed PFC's cybersecurity safeguards and pilfered the Private Information stored in PFC's systems.

28. Pursuant to a "Notice of Data Incident" posted on its website, PFC says that on February 26, 2022, PFC detected a "sophisticated ransomware attack in which an unauthorized third party accessed and disabled some of PFC's computer systems." *See* **Exhibit 3** (the "Breach Notice"). The Breach Notice says that PFC although "PFC found no evidence that personal information has been specifically misused," it that it "is possible that [Private Information' could have been accessed by an unauthorized third party." *Id.*

29. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information.

30. PFC had no effective means to quickly detect, prevent, stop, undo, or remediate the effects of the Data Breach, meaning cybercriminals could easily access and steal Private Information.

31. After the breach, PFC states it "immediately engaged third party forensic specialists to assist [] with securing the network environment and investigating the extent of any unauthorized activity." *Id.* PFC's "investigation determined that an unauthorized third party accessed filed containing certain individuals' personal information during this incident." *Id.*

32. But PFC disclosed little from its investigation. Indeed, the Breach Notice did not disclose or was unable to disclose *when* cybercriminals hacked its systems, *how* PFC allowed them to do so, *why* PFC was unable to stop it, and *what* information hackers obtained and from whom. Instead, PFC issued a bare-bones notice informing Data Breach victims that their highly sensitive Private Information may have been compromised.

33. On information and belief, PFC allowed the Data Breach to occur because it failed to train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over Private Information. PFC's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing Private Information. Further, the Breach Notice makes clear that PFC cannot, or will not, determine the full scope of the Data Breach, as it has been unable to determine exactly what information was stolen and when.

34. 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."[6]

c. Plaintiff's Experience

35. Mr. Skrabo does not know how PFC obtained his Private Information and he had never heard of PFC until he received a Breach Notice dated July 1, 2022 in July 2022. After receiving the Breach Notice, which was forwarded from an old address, Mr. Skrabo called the toll-free number in the notice and confirmed that he was a victim of the Data Breach.

---

[6] 5*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: July 23, 2022).

36. Plaintiff is very careful about sharing his sensitive Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

37. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

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

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

40. Plaintiff 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.

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

d. Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

42. Plaintiff and members of the proposed Class have suffered injury from the unauthorized access to, theft, and misuse of their Private Information that can be directly traced to Defendant.

43. As a result of PFC's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

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

b. The diminution in value of their Private Information;

c. The compromise and continuing publication of their Private Information;

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

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

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Private Information; and

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

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

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

46. In fact, the value of this highly sensitive Private Information is precisely why hackers targeted and stole it.

47. It can take victims years to spot identity or Private Information theft, giving criminals plenty of time to use that information for cash.

48. One such example of criminals using Private Information for profit is the development of "Fullz" packages.

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

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

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

51. Defendant disclosed the Private Information of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the Private Information of Plaintiff and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Private Information.

52. Defendant's failure to timely notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach.

e. PFC Failed to Adhere to FTC Guidelines

53. According to the FTC, unauthorized Private Information disclosures are extremely damaging to consumers' finances, credit history, and reputation, and can take time, money, and patience to resolve the fallout. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

54. According to the FTC, the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data

security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Private Information.

55. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

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

57. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

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

59. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations. *See In the matter of Lookout Services, Inc.*, No. C-4326, ⁋ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ⁋ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations.

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

f. PFC Failed to Adhere to HIPAA

61. The Health Insurance Portability and Accountability Act ("HIPAA") circumscribes security provisions and data privacy responsibilities designed to keep patients' medical

information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.

62. HIPAA provides specific privacy rules requiring comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of Private Information is properly maintained.

63. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic Private Information that it creates, receives, maintains, and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic Private Information in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic Private Information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendant workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic Private Information to allow access only to those

persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of Private Information in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard Private Information, in compliance with 45 C.F.R. § 164.530(c).

CLASS ACTION ALLEGATIONS

64. Plaintiff brings this action on behalf of himself and the proposed Class ("Class"), pursuant to Fed. R. Civ. P. 23(b)(2), (b)(3), and (c)(4):

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

All United States residents whose Private Information was compromised in the Data Breach disclosed by PFC in its Breach Notice.

66. In addition, Plaintiff seeks to represent the following class of Colorado residents:

All Colorado residents whose Private Information was compromised in the Data Breach disclosed by PFC in its Breach Notice.

67. Together, the Nationwide Class and Colorado Subclass are referred to as the "Class".

68. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

69. Plaintiff reserves the right to amend the class definition.

a. **Numerosity**. Plaintiff is representative of the proposed Class, which, on information and belief, numbers in the thousands, far too many to join in a single action;

b. **Typicality**. Plaintiff's claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

c. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. His interests do not conflict with Class members' interests and he has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

d. **Commonality**. Plaintiff and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's Private Information;

ii. 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;

iii. Whether Defendant was negligent in maintaining, protecting, and securing Private Information;

iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's Private Information;

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

vi. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vii. Whether Defendant's Breach Notice was reasonable;

viii. Whether the Data Breach caused Plaintiff and the Class injuries;

ix. What the proper damages measure is; and

x. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

70. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual class members are insufficient to make individual lawsuits economically feasible.

71. 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.

72. 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 Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiff 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 Plaintiff 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 Plaintiff 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 Plaintiff 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.

j. Whether Defendant complied with Colo. Rev. Stat. § 6-1-101, *et seq*.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

73. Plaintiff realleges all previous paragraphs as if fully set forth below.

74. Plaintiff and members of the Class entrusted their Private Information to Defendant. Defendant owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the Private Information in its care and custody, including implementing

industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

75. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their Private Information in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that Private Information —just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of the Class's Private Information by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the Private Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

76. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their Private Information. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

77. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security

protocols. Defendant actively sought and obtained Plaintiff' and members of the Class's personal information and Private Information.

78. The risk that unauthorized persons would attempt to gain access to the Private Information and misuse it was foreseeable. Given that Defendant holds vast amounts of Private Information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Private Information —whether by malware or otherwise.

79. Private Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Private Information of Plaintiff and members of the Class and the importance of exercising reasonable care in handling it.

80. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and Private Information of Plaintiff and members of the Class which actually and proximately caused the Data Breach and Plaintiff and members of the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

81. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's Private Information.

82. 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 customer information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the members of the Class's sensitive Private Information.

83. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and Class members' Private Information=and 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 Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

84. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

85. Defendant had a duty to Plaintiff and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff and the Class's Private Information.

86. Pursuant to HIPAA (42 U.S.C. § 1302d, et seq.), Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class members' Private Information.

87. Pursuant to HIPAA, Defendant had a duty to render the electronic Private Information it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as

specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 C.F.R. § 164.304 definition of encryption).

88. Plaintiff and Class members are within the class of persons that the HIPAA was intended to protect.

89. The harm that occurred as a result of the Data Breach is the type of harm that HIPAA was intended to guard against. The Federal Health and Human Services' Office for Civil Rights ("OCR") has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures relating to protected health information, caused the same harm as that suffered by Plaintiff and the Class members.

90. Had Plaintiff and members of the Class known that Defendant did not adequately protect their Private Information, Plaintiff and members of the Class would not have entrusted Defendant with their Private Information.

91. Defendant breached its duties to Plaintiff and the Class under HIPAA, by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

92. Defendant breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's Private Information.

93. Defendant's negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Private Information by criminals, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, and lost time and money incurred

to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Violation of Colorado Consumer Protection Act
(On Behalf of Plaintiff and the Class)

94. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

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

96. Plaintiff and the Class provided and/or entrusted sensitive and confidential Private Information to Defendant, which Defendant collected, stored, and maintained at its Colorado headquarters.

97. 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.

98. 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. Plaintiff and other members of the Class furnished or purchased these services. Plaintiff and the Class are actual or potential consumers as defined by Colo. Rev. Stat § 6-1-113(1), *et seq.*

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

100. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Private Information of Plaintiff and the 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.

101. 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 their security practices, and Plaintiff and the Class could not reasonably be expected to learn or discover the true facts.

102. 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 debt collection and payment services to consumers in violation of the Colorado Consumer Protection Act, 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 consumer's personal and financial information;

c. failing to disclose the material information, known at the time of the transaction – collection and retention of consumer Private Information to furnish debt collection and payment 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 its clients' customers' sensitive personal information from theft.

103. By engaging in the conduct delineated above, Defendant has violated the Colorado Consumer Protection Act 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 which 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 which 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.

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

105. 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 Plaintiff and the Class.

106. As a direct result of Defendant's violation of the Colorado Consumer Protection Act, Plaintiff and the Nationwide 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 remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect 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 Plaintiff and the Class.

107. As a result of Defendant's violation of the Colorado Consumer Protection Action, Plaintiff and the Nationwide 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 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's segment data by, among other things, creating firewalls and access controls so that if one area of Defendant 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 clients' customers' 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.

108. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices of Defendant alleged herein, Plaintiff 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 III
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

109. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

110. Plaintiff 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.

111. Defendant owed a duty to Plaintiff and Class Member to keep their Private Information confidential.

112. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiff's and Class Members' Private Information is highly offensive to a reasonable person.

113. Defendant's reckless and negligent failure to protect Plaintiff's and Class Members' Private Information constitutes an intentional interference with Plaintiff's 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.

114. Defendant's failure to protect Plaintiff's and Class Members' Private Information acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

115. Defendant knowingly did not notify Plaintiff's and Class Members in a timely fashion about the Data Breach.

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

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

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

119. Plaintiff 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 inability to safeguard the Private Information of Plaintiff and the Class.

120. Plaintiff, on behalf of himself and Class Members, seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' Private Information.

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

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

122. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

123. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable Private Information.

124. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information.

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

126. Plaintiff and Class members reasonably understood that Defendant would adequately protect the Private Information entrusted to it. Plaintiff and the proposed Class would

not have provided their Private Information, had they known Defendant would not adequately protect their Private Information.

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

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

129. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) 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 remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect 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 Plaintiff and Class Members.

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

131. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by it because of its misconduct and Data Breach.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about its data security practices and capabilities, the Data Breach and the stolen Private Information;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Dated: July 27, 2022

Respectfully Submitted,

/s/ Gary M. Klinger
Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
Email: gklinger@milberg.com

Samuel J. Strauss
sam@turkestrauss.com
Raina C. Borrelli
raina@turkestrauss.com
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Telephone (608) 237-1775
Facsimile: (608) 509-4423

Attorneys for Plaintiff and the Proposed Class