COMMONWEALTH OF KENTUCKY
16TH JUDICIAL CIRCUIT
KENTON CIRCUIT COURT
JUDGE _____
CASE NO. _____

Electronically filed

CHARLES VIVIALI, LISA ALICEA, and KAYLA LOFTON, individually, and on behalf of all others similarly situated — PLAINTIFFS

v. **CLASS ACTION COMPLAINT**

ONE POINT HR SOLUTIONS, LLC — DEFENDANT

* * * * * * * * * * * *

Plaintiffs Charles Viviali, Lisa Alicea, and Kayla Lofton ("Plaintiffs"), individually and on behalf of all similarly situated persons, bring this Amended Class Action Complaint against Defendant One Point HR Solutions, LLC ("Defendant" or "One Point") for its failure to properly secure and safeguard Representative Plaintiffs' and Class Members' private data.

I. INTRODUCTION

1. Plaintiffs bring this class action against One Point for its failure to properly secure and safeguard Plaintiff's and other similarly situated One Point customer's personally identifiable information ("PII") and protected health information ("PHI"), including names, social security numbers, dates of birth, driver's license numbers, state identification number, federal employer identification numbers, financial account information, government identification numbers, health insurance information, individual tac identification numbers, medical information, passport numbers, payment card information, email addresses, usernames, and passwords (the "Private Information"), from criminal hackers.

2. One Point, based in Covington, Kentucky, is a professional staffing organization that focuses on the warehouse, aviation, logistics, manufacturing,[1] and medical industries.

3. Recently, One Point filed official notice of a hacking incident with the Office of the Maine Attorney General.[2] Under state and federal law, organizations must report breaches involving PHI within at least sixty (60) days.

4. On or about September 6, 2024, One Point also sent out data breach letters (the "Notice") to individuals whose information was compromised as a result of the hacking incident.

5. Based on the Notice sent to Plaintiffs and "Class Members" (defined below), unusual activity was detected within some of One Point's email environment. In response, Defendant launched an investigation. One Point's investigation revealed that "an unknown unauthorized actor gained access to certain email accounts between July 3, 2023 and February 14, 2024 (the "Data Breach"). Yet, One Point waited 431 days to notify the public that they were at risk.

6. As a result of this delayed response, Plaintiffs and Class Members had no idea for months that 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.

7. The Private Information compromised in the Data Breach contained highly sensitive customer data, representing a gold mine for data thieves. The data included, but is not limited to, names, social security numbers, dates of birth, driver's license numbers, state identification number, federal employer identification numbers, financial account information,

[1] Home Page, ONE POINT HR SOLUTIONS, https://onepointhrs.com/ (last visited Nov. 4, 2024).
[2] *See* https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/1d70f976-a82c-4ad8-8584-2024152a3984.html (last visited December 29, 2025).

government identification numbers, health insurance information, individual tac identification numbers, medical information, passport numbers, payment card information, email addresses, usernames, and passwords that One Point collected and maintained.

8. Armed with the Private Information accessed in the Data Breach (and a head start), data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

9. There has been no assurance offered by One Point that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

10. Therefore, Plaintiffs and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

11. Plaintiffs bring this class action lawsuit to address One Point's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and its failure to provide timely and adequate notice to Plaintiffs and Class Members of the types of

information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

12. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to One Point, and thus One Point was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

13. Upon information and belief, One Point failed to properly monitor and implement security practices with regard to the computer network and systems that housed the Private Information. Had One Point properly monitored its networks, it would have discovered the Data Breach sooner.

14. Plaintiffs' and Class Members' identities are now at risk because of One Point's negligent conduct as the Private Information that One Point collected and maintained is now in the hands of data thieves and other unauthorized third parties.

15. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

II. PARTIES

16. Plaintiff, Charles Viviali, is a natural person and citizen of Florida where he intends to remain.

17. Plaintiff, Lisa Alicea, is a natural person and citizen of Missouri where she intends to remain.

18. Plaintiff, Kayla Lofton, is a natural person and citizen of Florida where she intends to remain.

19. Defendant One Point HR Solutions, LLC, is a limited liability company formed under the laws of Kentucky and its principal place of business at 118 W. Fifth Street, Suite 201, Covington, Kentucky 41011.3 Thus, under § 1332(d)(10) of CAFA, Defendant is citizen of Kentucky. Defendant is wholly and solely owned by Ronald Heineman, a citizen of Florida.

III. JURISDICTION AND VENUE

20. The Court has subject matter jurisdiction over this action pursuant to KRS § 23A.010.

21. This Court has jurisdiction over One Point because One Point operates in and/or is incorporated in this County.

22. Venue is proper in this Court pursuant to KRS § 452.460 because a substantial part of the events giving rise to this action occurred in this County and One Point has harmed Class Members residing in this County.

23. Pursuant to CR 8.01(2), the amount in controversy exceeds the minimum jurisdiction of the Kenton Circuit Court.

IV. FACTUAL ALLEGATIONS

A. One Point's Business and Collection of Plaintiff's and Class Members' Private Information

24. One Point is a professional staffing organization that focuses on the warehouse, aviation, logistics, manufacturing, and medical industries.[3] Defendant operates through several brands including Horizons HR Services, Elite Staffing Partners, Corporate Personnel Resources, C-Store Recruiting, Pivot Medical Staffing, Staffing Medical USA, Truline Drivers, and PPSR Solutions.[4]

[3] Home Page, ONE POINT HR SOLUTIONS, https://onepointhrs.com/ (last visited Nov. 4, 2024).
[4] *Our Brands,* ONE POINT HR SOLUTIONS, https://onepointhrs.com/our-brands/ (last visited Nov. 4, 2024).

25. As part of its business, Defendant receives and maintains the PII/PHI of thousands of its current and former customers and/or clients. In the ordinary course of receiving service from One Point, Plaintiffs and Class Members were required to provide their Private Information to Defendant.

26. In collecting and maintaining the PII/PHI, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiffs and Class Members themselves took reasonable steps to secure their PII/PHI

27. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, One Point assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

28. Plaintiffs and Class Members relied on One Point to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

B. The Data Breach and Defendant's Inadequate Notice to Plaintiffs and Class Members

29. For 226 days, Defendant was hacked in the Data Breach.[5] Worryingly, Defendant already admitted that "an unknown unauthorized actor gained access to certain email accounts between July 3, 2023 and February 14, 2024.[6]

30. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including names, social security numbers, dates of birth, driver's license numbers, state identification number, federal employer identification numbers,

[5] Notice of Potential Data Event, HORIZONS (Oct. 11, 2024) https://horizonshrservices.com/notice-of-potential-data-event/.
[6] *Id.*

financial account information, government identification numbers, health insurance information, individual tac identification numbers, medical information, passport numbers, payment card information, email addresses, usernames, and passwords.

31. On or about September 6, 2024, roughly 431 days after One Point learned that the Class's Private Information was first accessed by cybercriminals, One Point finally began to notify customers that its investigation determined that their Private Information was impacted.

32. One Point delivered Data Breach Notification Letters to Plaintiffs and Class Members, alerting them that their highly sensitive Private Information had been exposed.

33. Omitted from the Notice are crucial details like the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information is protected.

34. Thus, One Point's purported disclosure amounts to no real disclosure at all, as it fails to inform Plaintiffs and Class Members of the Data Breach's critical facts with any degree of specificity. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach was and is severely diminished.

35. In addition, the Notice offers no substantive steps to help victims like Plaintiffs and Class Members to protect themselves other than providing one year of credit monitoring – an offer that is woefully inadequate considering the lifelong increased risk of fraud and identity theft Plaintiffs and Class Members now face as a result of the Data Breach

36. One Point had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

37. Plaintiffs and Class Members provided their Private Information to One Point with the reasonable expectation and mutual understanding that One Point would comply with its obligations to keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

38. One Point's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

39. One Point knew or should have known that its electronic records would be targeted by cybercriminals.

C. One Point Failed to Comply with HIPAA

40. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep customer's 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.[7]

41. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII/PHI and PHI is properly maintained.[8]

42. Plaintiffs' and Class Members' Private Information compromised in the Data Breach included "protected health information" as defined by CFR § 160.103.

[7] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, inter alia: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[8] See 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

43. 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."

44. 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[.]"

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

46. Plaintiffs' and Class Members' unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

47. Based upon Defendant's Notice to Plaintiffs and Class Members, One Point reasonably believes that Plaintiffs' and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

48. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/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.

49. One Point reasonably believes that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/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.

50. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/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.

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

52. One Point reasonably believes that Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

53. It is reasonable to infer that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/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.

54. It should be rebuttably presumed that unsecured PHI acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

55. After receiving notice that they were victims of the Data Breach (which required the filing of a data 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 medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

56. In addition, One Point's Data Breach could have been prevented if One Point had implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its customers.

Filed 26-CI-00098 01/12/2026 John C. Middleton, Kenton Circuit Clerk

57. One Point's security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information One Point creates, receives, maintains, and transmits in violation of 45 CFR § 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR § 164.312(a)(1);

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

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR § 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR § 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR § 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 CFR § 164.306(a); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR §§ 164.502, *et seq.*

58. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 also required One Point to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***" (emphasis added).

59. Because One Point has failed to comply with HIPAA, while monetary relief may cure some of Plaintiffs' and Class Members' injuries, injunctive relief is also necessary to ensure One Point's approach to information security is adequate and appropriate going forward. One Point still maintains the PHI and other highly sensitive PII of its current and former customers, including Plaintiffs and Class Members. Without the supervision of the Court through injunctive relief, Plaintiffs' and Class Members' Private Information remains at risk of subsequent data breaches.

D. One Point Failed to Comply with FTC Guidelines

60. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the 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 Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

61. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[9] . 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. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

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

63. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by 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 FTCA, 15 U.S.C. §§ 45 *et seq*. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

64. Such FTC enforcement actions include those against businesses that fail to

[9] *Protecting Personal Information: A Guide for Business,* FEDERAL TRADE COMMISSION (October 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited on June 23, 2025).

adequately protect customer data, like One Point here. *See, e.g.*, *In the Matter of LabMD, Inc.*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

65. Section 5 of the FTCA, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like One Point of failing to use reasonable measures to protect Private Information they collect and maintain from consumers. The FTC publications and orders described above also form part of the basis of One Point's duty in this regard.

66. The FTC has also recognized that personal data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[10]

67. As evidenced by the Data Breach, One Point failed to properly implement basic data security practices. One Point'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 FTCA.

68. One Point was at all times fully aware of its obligation to protect the Private Information of its customers yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

[10] FTC Commissioner Pamela Jones Harbour, *Remarks Before FTC Exploring Privacy Roundtable* (Dec. 7, 2009), *transcript available at* https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited on June 23, 2025).

E. One Point Failed to Comply with Industry Standards

69. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

70. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[11]

71. The National Institute of Standards and Technology ("NIST") also recommends certain practices to safeguard systems, such as the following:

a. Control who logs on to your network and uses your computers and other devices.

b. Use security software to protect data.

c. Encrypt sensitive data, at rest and in transit.

d. Conduct regular backups of data.

e. Update security software regularly, automating those updates if

[11] *The 18 CIS Critical Security Controls*, CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/controls/cis-controls-list (last visited on June 23, 2025).

possible.

f. Have formal policies for safely disposing of electronic files and old devices.

g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

72. Further still, the United States Cybersecurity and Infrastructure Security Agency ("CISA") makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[12]

73. Defendant failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0

[12] *Shields Up: Guidance for Organizations*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/shields-guidance-organizations (last visited June 23, 2025).

(including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiffs' and Class Members' Private Information, resulting in the Data Breach.

F. One Point Breached its Duty to Safeguard Plaintiffs' and Class Members' Private Information

74. In addition to its obligations under federal and state laws, One Point owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. One Point owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

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

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect customers' Private Information;

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

d. Failing to sufficiently train its employees regarding the proper handling of its customers' Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to HIPAA and industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

76. One Point negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

77. Had One Point remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

78. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiffs and Class Members also lost the benefit of the bargain they made with One Point.

G. Plaintiffs and Class Members are at a Significantly Increased and Substantial Risk of Fraud and Identity Theft as a Result of the Data Breach.

79. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such

as data breaches or unauthorized disclosure of data.[13] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

80. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

81. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

82. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

---

[13] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on June 23, 2025).

Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

83. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

84. One such example of how malicious actors may compile Private Information is through the development of "Fullz" packages.

85. Cybercriminals can cross-reference two sources of the Private Information compromised in the Data Breach 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.

86. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and the proposed Class's phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen 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 Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class Members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

87. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[14] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

88. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

89. The Identity Theft Resource Center documents the multitude of harms caused by fraudulent use of PII in its 2023 Consumer Impact Report.[15] After interviewing over 14,000 identity crime victims, researchers found that as a result of the criminal misuse of their PII:

- 77-percent experienced financial-related problems;
- 29-percent experienced financial losses exceeding $10,000;
- 40-percent were unable to pay bills;

[14] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited June 23, 2025).

[15] *2023 Consumer Impact Report* (Jan. 2024), IDENTITY THEFT RESOURCE CENTER, *available online at*: https://www.idtheftcenter.org/wp-content/uploads/2023/08/ITRC_2023-Consumer-Impact-Report_Final-1.pdf (last visited on June 23, 2025).

- 28-percent were turned down for credit or loans;
- 37-percent became indebted;
- 87-percent experienced feelings of anxiety;
- 67-percent experienced difficulty sleeping; and
- 51-percent suffered from panic of anxiety attacks.[16]

90. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.[17]

91. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

92. While credit card information and associated PII can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute.[18]

93. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

94. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam

[16] *Id* at pp 21-25.

[17] Federal Trade Commission, *Warning Signs of Identity Theft, available at*: https://consumer.ftc.gov/articles/what-know-about-identity-theft (last visited on June 23, 2025).

[18] *Data Breaches: In the Healthcare Sector,* CENTER FOR INTERNET SECURITY, *available at*: https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited on June 23, 2025).

Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[19]

95. The ramifications of One Point's failure to keep its customers' Private Information secure are long lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

96. Here, not only was sensitive medical information compromised, but Social Security numbers were compromised too. The value of both PII and PHI is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

97. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[20]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

[19] Michael Ollove, "*The Rise of Medical Identity Theft in Healthcare*," KAISER HEALTH NEWS (Feb. 7, 2014), *available at*: https://kffhealthnews.org/news/rise-of-indentity-theft/ (last visited on June 23, 2025).

[20] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOVERNMENT ACCOUNTABILITY OFFICE (June 2007), *available at* https://www.gao.gov/assets/gao-07-737.pdf (last visited on June 23, 2025).

98. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

99. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

H. Plaintiffs' and Class Members' Damages

Plaintiff Lisa Alicea's Experiences and Injuries

100. Plaintiff Lisa Alicea is unsure how Defendant obtained—and later exposed—her PII/PHI. Regardless, Plaintiff Alicea received a personalized Data Breach notice explaining that her PII/PHI was exposed.

101. As a result, Plaintiff Alicea was injured by Defendant's Data Breach.

102. On information and belief, Defendant obtained Plaintiff Alicea's PII/PHI pursuant to Plaintiff Alicea's employment. Thus, on information and belief, as a condition of her employment, Defendant obtained her PII/PHI and used her PII/PHI to facilitate its business.

103. Plaintiff Alicea (or her third-party agent) provided her PII/PHI to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Alicea's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

104. Plaintiff Alicea (or her third-party agent) reasonably understood that a portion of the funds paid to Defendant (and/or derived from her employment) would be used to pay for adequate cybersecurity and protection of PII/PHI.

105. Plaintiff Alicea (or her third-party agent) is very careful about sharing her sensitive PII/PHI and stores any documents containing her PII/PHI in a safe and secure location. She (or her third-party agent) has never knowingly transmitted unencrypted sensitive PII/PHI in an unsecure manner over the internet or any other unsecured source. Plaintiff Alicea (or her third-party agent) would not have entrusted her PII/PHI to Defendant had she known of Defendant's lax data security policies.

106. Plaintiff Alicea received a Notice of Data Breach on October 11, 2024.

107. Thus, on information and belief, Plaintiff Alicea's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

108. Through its Data Breach, Defendant compromised Plaintiff Alicea's PII/PHI.

109. Plaintiff Alicea has *already* suffered from identity theft and fraud. For one, she received alerts from her Experian account that her data was found on the Dark Web.

110. Plaintiff Alicea received a flood of emails from banks and lenders notifying her of loan applications made under her name. Thus, it appears that cybercriminals have used Plaintiff Alicea's stolen PII/PHI to commit identity theft by applying for and obtaining fraudulent loans under Plaintiff Alicea's name. Thus far, Plaintiff Alicea has received the following notifications.

a. On November 5, 2024, Plaintiff Alicea received an email from "The Cardinal Program at Cloud Based Personal Loans" which notified her that "based on your recent application, you may be eligible for a $100-$40,000 loan."

b. On November 5, 2024, Plaintiff Alicea received an email from "MaxLoan365" which informed her that she was eligible for "anywhere from $100 to $7,599" in personal loans.

c. On November 6, 2024, Alicea received an email from "Prime Bank of America" informing her that "Your echeck of $1,825.00 is ready" and that "Estimated Deposit Date: Next Business Day."

d. On November 6, 2024, Plaintiff Alicea receiving an email from "LiveLaughFunds" which told her that "[y]our request for ($2800) has been verified" and "[t]hank you for choosing our services."

e. On November 6, 2024, Plaintiff Alicea received an email from "Blueview Lending" which notified her that her "Status" was "Verified" and that "Thank you for letting us help you with your financial goals."

f. On November 6, 2024, Plaintiff Alicea received an email from "Paywise" which reminded her to "complete your transaction by logging in and confirming your request today" as to obtain "funds up to $2,200[.]"

g. On November 7, 2024, Plaintiff Alicea received an email from "PrivateLenders.com" which informed her that "Lenders in our network are begging us for more opportunities to back borrowers like YOU" and "Click here to find your capital partner today."

h. On November 7, 2024, Plaintiff Alicea received another email from "Blueview Lending" which notified her that her "Status" was "Verified" and that "Thank you for letting us help you with your financial goals."

111. Plaintiff Alicea has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

112. Thus far, Plaintiff Alicea has spent 3–4 hours responding to the Data Breach including by researching the Data Breach and monitoring her accounts for suspicious activity.

113. And in the aftermath of the Data Breach, Plaintiff Alicea has suffered from a spike in spam and scam phone calls.

114. Plaintiff Alicea fears for her personal financial security and worries about what information was exposed in the Data Breach.

115. Because of Defendant's Data Breach, Plaintiff Alicea has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Alicea's injuries are precisely the type of injuries that the law contemplates and addresses.

116. Plaintiff Alicea suffered actual injury from the exposure and theft of her PII/PHI—which violates her rights to privacy.

117. Plaintiff Alicea suffered actual injury in the form of damages to and diminution in the value of her PII/PHI. After all, PII/PHI is a form of intangible property—property that Defendant was required to adequately protect.

118. Plaintiff Alicea suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Alicea's PII/PHI right in the hands of criminals.

119. Because of the Data Breach, Plaintiff Alicea anticipates spending considerable amounts of time and money to try and mitigate her injuries.

120. Today, Plaintiff Alicea has a continuing interest in ensuring that her PII/PHI—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Charles Viviali's Experiences

121. Plaintiff Charles Viviali is a former employee of Defendant.

122. Thus, Defendant obtained and maintained Plaintiff Viviali's PII/PHI.

123. As a result, Plaintiff Viviali was injured by Defendant's Data Breach.

124. As a condition of his employment with Defendant, Plaintiff Viviali provided Defendant with his PII/PHI. Defendant used that PII/PHI to facilitate its employment of Plaintiff Viviali, including payroll, and required Plaintiff Viviali to provide that PII/PHI in order to obtain employment and payment for that employment.

125. Plaintiff Viviali provided his PII/PHI to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Viviali's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

126. Plaintiff Viviali reasonably understood that a portion of the funds paid to Defendant (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of PII/PHI.

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

128. Plaintiff Viviali received a Notice of Data Breach dated October 11, 2024.

129. Thus, on information and belief, Plaintiff Viviali's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

130. Through its Data Breach, Defendant compromised Plaintiff Viviali's PII/PHI.

131. Plaintiff Viviali has spent -and will continue to spend- significant time and effort monitoring his accounts to protect himself from identify theft. After all, Defendant directed Plaintiff to take those steps in its breach notice. Since the breach occurred in July 2023 Plaintiff Viviali has spent at least ten hours monitoring his credit and identity, in addition to time spent investigating the circumstances around the Data Breach and obtaining legal counsel.

132. And in the aftermath of the Data Breach, Plaintiff Viviali has suffered from a spike in spam and scam emails and phone calls.

133. Plaintiff Viviali fears for his personal financial security and worries about what information was exposed in the Data Breach.

134. Because of Defendant's Data Breach, Plaintiff Viviali has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Viviali's injuries are precisely the type of injuries that the law contemplates and addresses.

135. Plaintiff Viviali suffered actual injury from the exposure and theft of his PII/PHI—which violates his rights to privacy.

136. Plaintiff Viviali suffered actual injury in the form of damages to and diminution in the value of his PII/PHI. After all, PII/PHI is a form of intangible property—property that Defendant was required to adequately protect.

137. Plaintiff Viviali suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's PII/PHI right in the hands of criminals.

138. Because of the Data Breach, Plaintiff Viviali anticipates spending considerable amounts of time and money to try and mitigate his injuries.

139. Today, Plaintiff Viviali has a continuing interest in ensuring that his PII/PHI—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Kayla Lofton's Experience and Injuries

140. Plaintiff Kayla Lofton is not positive how Defendant obtained—and later exposed—her PII/PHI. Regardless, Plaintiff Lofton received a personalized Data Breach notice explaining that her PII/PHI was exposed.[21]

141. As a result, Plaintiff Lofton was injured by Defendant's Data Breach.

142. On information and belief, Defendant obtained Plaintiff Lofton's PII/PHI pursuant to her employment with an employer who utilized One Point's services. Thus, on information and belief, as a condition of her employment, Defendant obtained Plaintiff Lofton's PII/PHI and used her PII/PHI to facilitate its business.

143. Plaintiff Lofton (or her third-party agent) provided her PII/PHI to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Lofton's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

[21] See Notice of Security Incident, October 11, 2024 attached as Exhibit A.

144. Plaintiff Lofton (or her third-party agent) reasonably understood that a portion of the funds paid to Defendant (and/or derived from her employment) would be used to pay for adequate cybersecurity and protection of PII/PHI.

145. Plaintiff Lofton (or her third-party agent) is very careful about sharing her sensitive PII/PHI and stores any documents containing her PII/PHI in a safe and secure location. She (or her third-party agent) has never knowingly transmitted unencrypted sensitive PII/PHI in an unsecure manner over the internet or any other unsecured source. Plaintiff Lofton (or her third-party agent) would not have entrusted her PII/PHI to Defendant had she known of Defendant's lax data security policies.

146. Plaintiff Lofton received Defendant's Notice of Security Incident on or about October 11, 2024, informing her that her Social Security Number and name were compromised in the Data Breach. Plaintiff Lofton signed-up for the credit monitoring offered therein.

147. Thus, on information and belief, Plaintiff Lofton's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

148. Through its Data Breach, Defendant compromised Plaintiff Lofton's PII/PHI.

149. Plaintiff Lofton has *already* suffered from identity theft and fraud due to the Data Breach, including a fraudulent charge to her Chase bank account by cybercriminals using the PII/PHI stolen in the Data Breach, requiring Plaintiff Lofton to receive a new debit card.

150. Plaintiff Lofton has spent—and will continue to spend—significant time and effort to mitigate the consequences of the Data Breach. After all, Defendant directed Plaintiff Lofton to take those steps in its breach notice.

151. Thus far, Plaintiff Lofton has spent 7-8 hours responding to the Data Breach, including researching the Data Breach, disputing the fraudulent charge, and monitoring her accounts for suspicious activity.

152. Moreover, in the aftermath of the Data Breach, Plaintiff Lofton has suffered a dramatic increase in spam and scam phone calls.

153. Plaintiff Lofton fears for her personal financial security and worries about what information was exposed in the Data Breach.

154. Because of Defendant's Data Breach, Plaintiff Lofton has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Lofton's injuries are precisely the type of injuries that the law contemplates and addresses.

155. Plaintiff Lofton suffered actual injury from the exposure and theft of her PII/PHI—which violates her rights to privacy.

156. Plaintiff Lofton suffered actual injury in the form of damages to and diminution in the value of her PII/PHI. After all, PII/PHI is a form of intangible property—property that Defendant was required to adequately protect.

157. Plaintiff Lofton suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Lofton's PII/PHI right in the hands of criminals.

158. Because of the Data Breach, Plaintiff Lofton anticipates spending considerable amounts of time and money to try and mitigate her injuries.

159. Today, Plaintiff Lofton has a continuing interest in ensuring that her PII/PHI—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

V. CLASS ACTION ALLEGATIONS

160. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Ky. CR Rule 23.01 and 23.02.

161. Specifically, Plaintiffs propose the following Kentucky Class definition (referred to herein as the "Class"), subject to amendment as appropriate:

> **Kentucky Class**
>
> All citizens of the state of Kentucky who had Private Information impacted as a result of the Data Breach, including all who were sent a notice of the Data Breach.
>
> **Nationwide Class**
>
> All individuals residing in the United States whose PII/PHI was compromised in the Data Breach that began in July 2023 and impacted One Point HR Solution, LLC including all those individuals who received notice of the breach.

162. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

163. Plaintiffs reserve the right to modify or amend the definition of the proposed Kentucky Class, as well as add subclasses, if necessary, before the Court determines whether certification is appropriate.

164. The proposed Class meets the criteria for certification under Ky. CR Rule 23.02(a), (b), and (c).

165. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of thousands of customers of One Point whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through One Point's records, Class Members' records, publication notice, self-identification, and other means.

166. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether One Point engaged in the conduct alleged herein;

b. Whether One Point's conduct violated the FTCA and HIPAA;

c. When One Point learned of the Data Breach

d. Whether One Point's response to the Data Breach was adequate;

e. Whether One Point unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;

f. Whether One Point failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

g. Whether One Point's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether One Point's data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether One Point owed a duty to Class Members to safeguard their Private Information;

j. Whether One Point breached its duty to Class Members to safeguard their Private Information;

k. Whether hackers obtained Class Members' Private Information via the Data Breach;

l. Whether One Point had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

m. Whether One Point breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

n. Whether One Point knew or should have known that its data security systems and monitoring processes were deficient;

o. What damages Plaintiffs and Class Members suffered as a result of One Point's misconduct;

p. Whether One Point's conduct was negligent;

q. Whether One Point's conduct was *per se* negligent;

r. Whether One Point was unjustly enriched;

s. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

167. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of One Point. Plaintiffs are advancing the same claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

168. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

169. Predominance. One Point has engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from One Point's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

170. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class

Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for One Point. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

171. Class certification is also appropriate under Ky. CR Rule 23.02(b). One Point has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

172. Finally, all members of the proposed Class are readily ascertainable. One Point has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by One Point.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

173. Plaintiffs restate and realleges all of the allegations stated above as if fully set forth herein.

174. One Point knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

175. One Point's duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

176. One Point knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. One Point was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

177. One Point owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. One Point's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect customers' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to HIPAA and the FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

178. One Point's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . .

practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

179. One Point's duty also arose because Defendant was bound by industry standards to protect its customers' confidential Private Information.

180. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and One Point owed them a duty of care to not subject them to an unreasonable risk of harm.

181. One Point, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within One Point's possession.

182. One Point, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

183. One Point, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

184. One Point breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA; and

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

185. One Point acted with reckless disregard for the rights of Plaintiffs and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiffs and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

186. One Point had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust One Point with their Private Information was predicated on the understanding that One Point would take adequate security precautions. Moreover, only One Point had the ability to protect its systems (and the Private Information that it stored on them) from attack.

187. One Point's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised and exfiltrated as alleged herein.

188. One Point's breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

Filed 26-CI-00098 01/12/2026 John C. Middleton, Kenton Circuit Clerk

189. As a result of One Point's negligence in breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

190. One Point also had independent duties under state laws that required it to reasonably safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Breach.

191. As a direct and proximate result of One Point's negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

192. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

193. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

194. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring One Point to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

195. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

196. Pursuant to Section 5 of the FTCA, One Point had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and Class Members.

197. Pursuant to HIPAA, 42 U.S.C. §§ 1302(d), *et seq.*, One Point had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information.

198. Specifically, pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

199. One Point breached its duties to Plaintiffs and Class Members under the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

200. Specifically, One Point breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

201. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII and PHI (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of One Point's duty in this regard.

202. One Point also violated the FTCA and HIPAA by failing to use reasonable measures to protect the Private Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

203. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to One Point's networks, databases, and computers that stored Plaintiffs' and Class Members' unencrypted Private Information.

204. Plaintiffs and Class Members are within the class of persons that the FTCA and HIPAA are intended to protect, and One Point's failure to comply with both constitutes negligence *per se*.

205. Plaintiffs' and Class Members' Private Information constitutes personal property that was stolen due to One Point's negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

206. As a direct and proximate result of One Point's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

207. As a direct and proximate result of One Point's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

208. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring One Point to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

209. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

210. One Point provides services to Plaintiffs and Class Members. Plaintiffs and Class Members formed an implied contract with Defendant regarding the provision of those services through their collective conduct, including by Plaintiffs and Class Members paying for services and/or entrusting their valuable Private Information to Defendant in exchange for such services.

211. Through Defendant's sale of services to Plaintiffs and Class Members, it knew or should have known that it must protect Plaintiffs' and Class Members' confidential Private Information in accordance with its policies, practices, and applicable law.

212. As consideration, Plaintiffs and Class Members paid money to One Point and/or turned over valuable Private Information to One Point. Accordingly, Plaintiffs and Class Members bargained with One Point to securely maintain and store their Private Information.

213. One Point accepted payment and/or possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services to Plaintiffs and Class Members.

214. In paying Defendant and/or providing their valuable Private Information to Defendant in exchange for Defendant's services, Plaintiffs and Class Members intended and understood that One Point would adequately safeguard Private Information as part of those services.

215. Defendant's implied promises to Plaintiffs and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that

is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; (7) complying with HIPAA standards to make sure that Plaintiffs' and Class Members' PHI would remain protected; and (8) taking other steps to protect against foreseeable data breaches.

216. Plaintiffs and Class Members would not have entrusted their Private Information to One Point in the absence of such an implied contract.

217. Had One Point disclosed to Plaintiffs and the Class that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and Class Members would not have provided their Private Information to One Point.

218. One Point violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Private Information. One Point further breached these implied contracts by failing to comply with its promise to abide by HIPAA.

219. Additionally, One Point breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information it created, received, maintained, and transmitted, in violation of 45 CFR § 164.306(a)(1).

220. One Point also breached the implied contracts with Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic systems that maintain

electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 CFR § 164.312(a)(1).

221. One Point further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR § 164.308(a)(1).

222. One Point further breached the implied contracts with Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR § 164.308(a)(6)(ii).

223. One Point further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR § 164.306(a)(2).

224. One Point further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR § 164.306(a)(3).

225. One Point further breached the implied contracts with Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations, in violation of 45 CFR § 164.306(a).

226. One Point further breached the implied contracts with Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR §§ 164.502, *et seq.*

227. One Point further breached the implied contracts with Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in violation of 45 CFR § 164.530(c).

228. One Point further breached the implied contracts with Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PHI.

229. A meeting of the minds occurred, as Plaintiffs and Class Members agreed, *inter alia*, to provide payment and/or accurate and complete Private Information to One Point in exchange for One Point's agreement to, *inter alia*, provide services that included protection of their highly sensitive Private Information.

230. Plaintiffs and Class Members have been damaged by One Point's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT IV
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

231. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

232. This Count is pleaded in the alternative to Count III above.

233. Plaintiffs and Class Members conferred a benefit on One Point by turning over their Private Information to Defendant and by paying for services that should have included cybersecurity protection to protect their Private Information. Plaintiffs and Class Members did not receive such protection.

234. Upon information and belief, One Point funds its data security measures entirely from its general revenue, including from payments made to it by Plaintiffs and Class Members.

235. As such, a portion of the payments made by Plaintiffs and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to One Point.

236. One Point has retained the benefits of its unlawful conduct, including the amounts of payment received from Plaintiffs and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

237. One Point knew that Plaintiffs and Class Members conferred a benefit upon it, which One Point accepted. One Point profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiffs' and Class Members' Private Information and prevented the Data Breach.

238. If Plaintiffs and Class Members had known that One Point had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

239. Due to One Point's conduct alleged herein, it would be unjust and inequitable under the circumstances for One Point to be permitted to retain the benefit of its wrongful conduct.

240. As a direct and proximate result of One Point's conduct, Plaintiffs and Class Members have suffered, and/or are at a continued, imminent risk of suffering, injury that includes but is not limited to the following: (i) the loss of the opportunity to control how their Private Information is used; (ii) the compromise, publication, and/or theft of their Private Information;

(iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in One Point's possession and is subject to further unauthorized disclosures so long as One Point fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vi) 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.

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

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

COUNT V
BREACH OF FIDUCIARY DUTY
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

243. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

244. In light of the special relationship between One Point and its customers, whereby One Point became a guardian of Plaintiffs' and Class Members' Private Information (including highly sensitive, confidential, personal, and other PHI) One Point was a fiduciary, created by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its customers, including Plaintiffs and Class Members. This benefit included (1) the safeguarding of Plaintiffs' and Class Members' Private Information; (2) timely notifying Plaintiffs and Class Members of the Data Breach; and (3) maintaining complete and accurate records of what and where One Point's customers' Private Information was and is stored.

245. One Point had a fiduciary duty to act for the benefit of Plaintiffs and the Class upon matters within the scope of its customers' relationship, in particular to keep the Private Information secure.

246. One Point breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently investigate the Data Breach to determine the number of Class Members affected and notify them within a reasonable and practicable period of time.

247. One Point breached its fiduciary duties to Plaintiffs and the Class by failing to protect their Private Information.

248. One Point breached its fiduciary duties to Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic PHI One Point created, received, maintained, and transmitted, in violation of 45 CFR § 164.306(a)(1).

249. One Point breached its fiduciary duties to Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 CFR § 164.312(a)(1).

250. One Point breached its fiduciary duties to Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR § 164.308(a)(1).

251. One Point breached its fiduciary duties to Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR § 164.308(a)(6)(ii).

252. One Point breached its fiduciary duties to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 CFR § 164.306(a)(2).

253. One Point breached its fiduciary duties to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR § 164.306(a)(3).

254. One Point breached its fiduciary duties to Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce, in violation of 45 CFR § 164.306(a).

255. One Point breached its fiduciary duties to Plaintiffs and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 CFR §§ 164.502, *et seq.*

256. As a direct and proximate result of One Point's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer the harms and injuries

alleged herein, as well as anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above, seeks the following relief:

A. An order certifying this action as a Class action under Ky. CR Rule 23.02, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are a proper representative of the Class requested herein;

B. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

C. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

D. An order instructing One Point to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

E. An order requiring One Point to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

F. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

G. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: January 12, 2026

Respectfully submitted,

/s/ Andrew E. Mize

Andrew E. Mize (KY Bar No. 94453)
J. Gerard Stranch, IV (*pro hac vice* forthcoming)
Grayson Wells (*pro hac vice* forthcoming)
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
amize@stranchlaw.com

Daniel Srourian (*pro hac vice* forthcoming)
SROURIAN LAW FIRM, P.C.
468 N. Camden Dr., Suite 200
Beverly Hills, California 90210
(213) 474-3800
(213) 471-4160 (facsimile)
daniel@slfla.com

Raina C. Borrelli (*pro hac vice* forthcoming)
Samuel J. Strauss (*pro hac vice* forthcoming)
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago Illinois, 60611
(872) 263-1100
(872) 263-1109 (facsimile)
raina@straussborrelli.com
sam@straussborrelli.com

Counsel for Plaintiffs and the Proposed Class

Filed 26-CI-00098 01/12/2026 John C. Middleton, Kenton Circuit Clerk

This page was intentionally left blank

EXHIBIT A

Filed 26-CI-00098 01/12/2026 John C. Middleton, Kenton Circuit Clerk

One Point
—HR SOLUTIONS—
P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: STN2HSZVYB
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

Kayla Lofton
[redacted]

October 11, 2024

NOTICE OF SECURITY INCIDENT

Dear Kayla Lofton:

One Point HR Solutions, Inc. ("One Point") writes to inform you of an event involving some of your personal information. Safeguarding information is among One Point's highest priorities, and this letter provides details of the event, our response to it, and resources available to you to help protect your information from possible misuse, should you feel it appropriate to do so.

What Happened? One Point recently became aware of suspicious activity in our email environment. We quickly launched an internal investigation and engaged third-party forensic and data privacy specialists to investigate the nature and scope of the activity. The investigation determined that an unknown unauthorized actor(s) gained access to certain email accounts between July 5, 2023 and February 14, 2024. We then undertook a comprehensive and time-intensive review of the potentially impacted data with the assistance of additional data privacy specialists to identify the information contained within, identify the individuals whose information may have been impacted, and identify accurate address information for potentially impacted individuals. On September 9, 2024, One Point completed this review and determined that the email accounts contained information related to you. One Point is notifying you out of an abundance of caution because, although there is no evidence that the unknown unauthorized actor(s) actually saw or acquired information related to you, the investigation determined that certain information related to you may have been accessed or acquired by an unknown unauthorized actor(s).

What Information Was Involved? Our investigation determined that [illegible] be affected [illegible] Social Security number and name. Again, One Point is unaware [illegible] or actual misuse of [illegible] information.

What We Are Doing. [illegible] confidentiality, privacy, and security of information in our care [illegible] the nature and [illegible] of the suspicious activity, we quickly commenced [illegible] and are cooperating [illegible] Further, we promptly reported the event to federal and local law enforcement [illegible] and have implemented additional cybersecurity [illegible] investigations [illegible] moving forward. [illegible] reinforced with our staff the importance of measures to further [illegible] and worked with numerous data privacy specialists to assist in the response. safeguarding information in our care [illegible] undertook a robust effort to review the potentially impacted data to ensure we could notify any [illegible] impacted individuals [illegible] to best protect the information, should they feel it appropriate to do so.