IN THE CHANCERY COURT FOR THE TWENTIETH JUDICIAL DISTRICT
DAVIDSON COUNTY, TENNESSEE

KAREN LYTLE, individually, and on behalf of all others similarly situated, **Plaintiff,** **v.** **REVANCE THERAPEUTICS, INC.** **Defendant.**	Case No. _____

CLASS ACTION COMPLAINT AND JURY DEMAND

Plaintiff, KAREN LYTLE, individually, and on behalf of all others similarly situated (hereinafter, "Plaintiff"), brings this Class Action Complaint, against Defendant, REVANCE THERAPEUTICS, INC. ("Revance" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, members, and/or other related entities, and upon personal knowledge as to her own actions, and information and belief as to all other matters, alleges as follows:

INTRODUCTION

1. This action arises out of the public exposure of the confidential, private information of Revance's current and former employees, Personally Identifying Information[1] ("PII") and Protected Health Information ("PHI") (collectively "Private Information"), Plaintiff and the Class

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8). To be clear, according to Defendant, not every type of information included in that definition was compromised in the Data Breach.

Members, from March 15, 2023 to April 10, 2023 during a cyberattack, caused by Defendant's failures to adequately safeguard that information ("the Data Breach").

2. According to Defendant, the Private Information unauthorizedly disclosed in the Data Breach includes employees' names, Social Security numbers, and health or health insurance information[2] as well as Financial Account Number or Credit/Debit Card Number (in combination with security code, access code, password or PIN for the account).[3]

3. Founded in 2002, Revance is a biotechnology company headquartered in Nashville, Tennessee, with approximately $78 million in revenue in 2021 and five hundred (500) employees.[4]

4. As a condition of working for Revance, Defendant required its employees to provide it with their sensitive Private Information, which Revance promised to protect from unauthorized disclosure.

5. Defendant failed to undertake adequate measures to safeguard the Private Information of Plaintiff and the proposed Class Members, including failing to implement industry standards for data security, and failing to properly train employees on cybersecurity protocols, resulting in the Data Breach.

6. Although Defendant purportedly discovered the Data Breach on April 9, 2023, it failed to immediately notify and warn current and former employees who were victimized in the breach, waiting until July 10, 2023 to send written notice to Plaintiff and the Class Members.[5]

7. As a direct and proximate result of Defendant's failures to protect current and

---

[2] Revance Notice of Data Breach, July 10, 2023 ("Data Breach Notice"), **attached as Exhibit A.**
[3] Revance Data Breach Notification to Maine Attorney General, July 10, 2023, available at https://apps.web.maine.gov/online/aeviewer/ME/40/f8e0d43b-9a45-49e9-ae01-976b9ad1a72b.shtml
[4] *See* Revance website, "About Revance," avail. at https://www.revance.com/company/about-revance/ (last accessed August 11, 2023).
[5] *See* Data Breach Notice, Exhibit A.

former employees' sensitive Private Information and warn them promptly and fully about the Data Breach, Plaintiff and the proposed Class Members have suffered widespread injury and damages necessitating Plaintiff to seek relief on a class wide basis.

PARTIES

8. Plaintiff is a natural person and resident and citizen of the State of Nebraska, residing in Louisville, Cass County, Nebraska, where she intends to remain. Plaintiff is a former Revance employee and Data Breach victim.

9. Revance is a corporation organized and existing under the laws of the State of Delaware with a principal place of business at 1222 Demonbreun Street, Suite 1001 in Nashville, Davidson County, Tennessee 37203.

JURISDICTION & VENUE

10. This Court has general jurisdiction over this action under T.C.A. § 16-10-101.

11. This Court has personal jurisdiction over Defendant because it resides and operates in this state.

12. Venue is proper in this Court under T.C.A. § 20-4-101 because Revance resides in Davidson County, and the cause of action arose in this County.

BACKGROUND FACTS

A. Defendant Fails to Safeguard Employees' Private Information

13. Revance is a publicly traded biotechnology company headquartered in Nashville, Tennessee which holds itself out as "setting the new standard in healthcare by elevating patient and physician experiences through the development, acquisition and commercialization of innovative aesthetic and therapeutic offerings," and with a "deep experience commercializing

products for large pharmaceutical companies in highly competitive markets…"[6]

14. Revance researches, develops and manufactures pharmaceuticals for aesthetic and therapeutic purposes, including Daxxify (DaxibotulinumtoxinA-lanm), "the first and only peptide formulated neuromodulator with long-lasting results, [] FDA approved for the temporary improvement of moderate to severe frown lines (glabellar lines) in adults[,]" and under regulatory review for therapeutic treatment of Cervical Dystonia; and the RHA Collection, "…Resilient Hyaluronic Acid, [] the only hyaluronic acid (HA) filler approved by the FDA for dynamic facial lines, wrinkles and folds that are moderate to severe…"[7]

15. In addition, Revance provides services such as "Opul," a "unique financial technology platform designed to transform existing payment processing ecosystems and improve both aesthetic economics and patient experiences."[8]

16. Revance reports having total revenue of $78 million[9] and $58.1 million total revenue for the second quarter ending June 30, 2023.[10]

17. As a condition of employment, Revance requires that its employees provide it with massive amounts of their Private Information.

18. Revance collects and stores this Private Information on its information technology computer systems, on information and belief located at its headquarters in Nashville, Tennessee.

19. Indeed, as set forth in Revance's California Privacy Policy for Employees and Contingent Workers – Notice of Collection of Personal Information (Privacy Notice) ("Privacy

---

[6] https://www.revance.com/company/about-revance/ (last accessed August 11, 2023).
[7] https://www.revance.com/products/ (last acc. August 11, 2023); https://www.revance.com/therapeutics/
[8] https://www.revance.com/products/ (last accessed August 11, 2023)
[9] https://www.revance.com/company/about-revance/
[10] https://investors.revance.com/news-releases/news-release-details/revance-reports-second-quarter-2023-financial-results-provides

Policy," Exhibit B), Defendant requires that its employees provide their "[f]ull name[s], nicknames or previous names (such as maiden names) [;] [h]onorifics and titles, preferred form of address [;] [m]ailing address[es][;] [e]mail address[es][;] [p]hone numbers[;] [c]ontact information for related persons, such as authorized users of [their] account[s]" as well as Social Security numbers, Driver's license numbers, Passport numbers, "other government-issued identifiers…"[11]

20. Further, Defendant collects employees' financial information such as bank account numbers, payment card information, credit reports, credit score, and financial information related to employee benefits.[12]

21. In addition, Revance requires that its employees provide, and collects, their health information and health insurance information, including:

> …medical treatment or diagnosis, medicines taken, and other health values and sensor readings • Drug allergies • Name/Contact of healthcare providers • Health insurance company • Insurance account number • Information on payment for healthcare services (EOB forms, HSA statements, claims data, claims assistance records) • Health plan beneficiary names/numbers • Information needed to accommodate disabilities • Information about workplace accidents and occupational safety
>
> […and "Health Insurance Data" of] • Policy Number • Reimbursement Data • Co-pay data • Coverage amount data • Health values, sensor reading data (e.g., HBA1C,blood glucose, etc.) • Subscriber or Account identification number • Claims history • Benefits information…[13]

22. When Defendant collects this Private Information, it promises to protect and safeguard the information from unauthorized disclosure.

---

[11] Revance, "California Privacy Policy for Employees and Contingent Workers – Notice of Collection of Personal Information (Privacy Notice)," Effective Date December 14, 2021, avail. at https://www.revance.com/wp-content/uploads/2023/01/CCPA-Privacy-Policy-Employees-and-Contingent-Workers-Final-1.pdf, **attached as Exhibit B.**

[12] *Id*.

[13] *Id*.

23. In Revance's Code of Business Conduct and Ethics, it states:

> **Employees who have received or have access to confidential information should take care to keep this information confidential. Confidential information includes […] personally identifiable information pertaining to employees, patients, customers or other individuals** (including, for example, names, addresses, telephone numbers and social security numbers), and similar types of information provided to us by our customers, suppliers and partners.[14]

24. Defendant's Code of Business Conduct and Ethics goes onto say that, "[e]very employee has a duty to refrain from disclosing to any person confidential or proprietary information about us or any other company learned in the course of employment here, until that information is disclosed to the public through approved channels."[15]

25. Moreover, in the Code of Business Conduct and Ethics, Revance requires that, "[i]f your job entails access to personal information, including but not limited to protected health information, contact details, financial information, or transaction data, you must take appropriate measures to safeguard that information. Sharing personal data with any external parties or internal parties without a legitimate business need is prohibited." […] "All permitted uses of personal information are outlined in our privacy policies."[16]

26. Revance's Privacy Policy (Exhibit B) enumerates the purposes under which Private Information may be disclosed, e.g., for background checks, to identify employees, and for "Everyday Business Purposes," such as "contract management, analytics, fraud prevention, corporate governance, reporting, legal compliance and to fulfill our legal obligations, and to protect our rights and the rights and safety, including the health safety, of employees, contractors,

---

[14] Code of Business Conduct and Ethics, rev. Dec. 6, 2022, "10. Confidentiality," avail. at https://investors.revance.com/static-files/7b167543-8b03-4083-94f5-be24034a112b (last acc. Aug. 11, 2023) (emphasis added), **attached as Exhibit C.**

[15] *Id.*

[16] *Id.*, "11. Privacy."

and others."[17]

27. None of the permitted purposes for Revance's collection and use of employee Private Information in Defendant's Privacy Policy include the Data Breach.

28. Revance represented to its employees that it would take adequate measures to safeguard their Private Information.

29. Despite this, Defendant does not follow industry standard practices in securing employees' Private Information.

30. According to Defendant's Data Breach Notice to affected victims:

> On April 9, 2023, we discovered that an unauthorized third party had accessed and exfiltrated information from certain Revance systems. We immediately began an investigation to determine the scope of and contain the incident. Based on our investigation, the incident occurred between March 15, 2023 and April 10, 2023. After additional analysis, on April 27, 2023, we confirmed that the third party accessed and exfiltrated certain personal information from Revance's systems.[18]

31. Revance's Data Breach Notice went onto explain that after discovering the Data Breach, it "…terminated the third party's access to the affected systems," notified law enforcement, and took "steps to enhance the security controls used to help protect your data."[19]

32. Despite learning of the Data Breach on April 9, 2023, Revance waited three (3) months until July 10, 2023 to inform affected current and former employees, including Plaintiff and the Class Members, of the unauthorized disclosure of their Private Information in the Data Breach, which it did by written letter. *See* Exhibit A.

33. The Data Breach Notice went on to state Revance was not aware of any misuse of the Private Information that was exfiltrated and stolen by cybercriminals, but nevertheless encouraged affected current and former employees to "remain vigilant for incidents of fraud and

[17] Privacy Policy, Exhibit B.
[18] Data Breach Notice, Exhibit A.
[19] *Id*.

identity theft, including by regularly reviewing your account statements and monitoring free credit reports," and to report suspicious activity, identity theft, or fraud to their financial institutions.[20]

34. Revance's Data Breach Notice further apprised Data Breach victims of their abilities to put a fraud alert or security freeze on their credit files.[21]

35. Further, in the Data Breach Notice, Defendant offered affected victims two (2) years of identity monitoring services through Kroll.[22]

36. On the same date as the Data Breach Notice, July 10, 2023, Revance reported the Data Breach to the Maine Attorney General, providing more information concerning the Data Breach than it provided the actual victims, Plaintiff and the Class Members. In fact, Defendant told the Maine Attorney General that the Data Breach occurred because of an external system breach (hacking) attack; and, that following its analysis completed on April 27, 2023, it conducted a review of the exfiltrated data and identification of impacted individuals, completed on June 15, 2023, and determined that the Data Breach, "was caused by the compromise of an employee's credentials."[23]

37. Moreover, Revance's Data Breach notification to the Maine Attorney General disclosed that 2,803 individuals were impacted in the Data Breach.[24]

38. Plaintiff's and the proposed Class Members' Private Information was unauthorizedly disclosed to third-party cybercriminals in Defendant's Data Breach, including their

---

[20] *Id*.
[21] *Id*.
[22] *Id*.
[23] Revance Data Breach Notification to Maine Attorney General, July 10, 2023, available at https://apps.web.maine.gov/online/aeviewer/ME/40/f8e0d43b-9a45-49e9-ae01-976b9ad1a72b.shtml
[24] *Id*.

names, Social Security numbers, and health or health insurance information[25] as well other identifiers, Financial Account Numbers or Credit/Debit Card Numbers (in combination with security code, access code, password or PIN for the account).[26]

39. Defendant's conduct, by acts of commission or omission, caused the Data Breach, including: Revance's failures to implement best practices and comply with industry standards concerning computer system security to adequately safeguard Private Information, allowing Private Information to be accessed and stolen, by failing to implement security measures that could have prevented, mitigated, or timely detected the Data Breach, and by failing to adequately train its employees on cybersecurity policies, enforce those policies, or maintain reasonable security practices and systems, resulting in the Data Breach.

40. On information and belief, as more fully articulated below, Plaintiff and the members of the proposed Class Members' Private Information, unauthorizedly disclosed to third-party cybercriminals in the Data Breach, has now or will imminently be posted to the Dark Web for public viewing and use, in the public domain, and utilized for criminal purposes and fraudulent misuse.

B. Plaintiff's Experience

41. Plaintiff was an employee of Revance in 2014 as a paralegal.

42. As a condition of employment with Defendant, Plaintiff was required to provide her Private Information to Revance, including but not limited to her name, Social Security number, and health or health insurance information.

---

[25] Revance Notice of Data Breach, July 10, 2023 ("Data Breach Notice"), **attached as Exhibit A.**

[26] Revance Data Breach Notification to Maine Attorney General, July 10, 2023, available at https://apps.web.maine.gov/online/aeviewer/ME/40/f8e0d43b-9a45-49e9-ae01-976b9ad1a72b.shtml

43. In entrusting her Private Information to Defendant as a condition of being employed with Revance, Plaintiff believed that Revance would adequately safeguard that information, including as set forth in its privacy policies. Had Plaintiff known that Revance did not utilize reasonable data security measures, Plaintiff would not have entrusted her Private Information to Defendant.

44. Plaintiff received Defendant's Data Breach Notice dated July 10, 2023, informing him that her Private Information, including her name, Social Security number, and health or health insurance information, was unauthorizedly disclosed to and exfiltrated by cybercriminals in Revance's Data Breach.

45. Plaintiff enrolled in the identity monitoring services with Kroll offered by Defendant.

46. As a direct and proximate result of the Data Breach permitted to occur by Defendant, Plaintiff has suffered, and imminently will suffer, injury-in-fact and damages, including the unauthorized disclosure of the Private Information itself, which, on information and belief due to the nature of the cyberattack, has been or imminently will be posted on the dark web for sale and used for criminal and fraudulent purposes.

47. In addition, as a result of the Data Breach Plaintiff has been and will be forced to expend considerable time and effort to monitor her accounts and credit files to protect herself from identity theft and fraudulent misuse of her Private Information disclosed in the Data Breach.

48. Furthermore, Plaintiff has been caused significant worry and feelings of anxiety and emotional distress regarding the disclosure of her Private Information in the Data Breach.

49. Had Plaintiff known that Defendant did not adequately protect her Private Information, she would not have entrusted her sensitive Private Information to Revance.

50. Furthermore, Plaintiff's sensitive Private Information remains in Defendant's possession in its computer systems without adequate protection against known threats, exposing Plaintiff to future breaches and additional harm.

51. As a result of Revance's Data Breach, its victims face a lifetime risk of identity theft, as it includes sensitive information that cannot be changed, like their Social Security numbers. Accordingly, the identity theft protection which Defendant offered is wholly insufficient to compensate Plaintiff and the Class Members for their damages resulting therefrom.

C. This Data Breach was Foreseeable by Defendant.

52. Plaintiff and the proposed Class Members provided their Private Information to Defendant as a condition of employment with the reasonable expectation and mutual understanding that Defendant would comply with their obligations to keep such information confidential and secure from unauthorized access.

53. By failing to do so, Defendant put all Class Members at risk of identity theft, financial fraud, and other harms.

54. Defendant tortiously, or in breach of their implied contracts, failed to take the necessary precautions required to safeguard and protect the Private Information of Plaintiff and the Class Members from unauthorized disclosure. Defendant's actions represent a flagrant disregard of Plaintiff's and the other Class Members' rights.

55. Plaintiff and Class Members were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing Private Information and the critical importance of providing adequate security for that information.

56. According to the ITRC's January 2023 report for 2022, "[t]he number of publicly

reported data compromises in the U.S. totaled 1,802 in 2022. This represents the second highest number of data events in a single year and just 60 events short of matching 2021's all-time high number of data compromises."[27] In 2022, there were approximately 422 million individuals affected by cyberattacks.[28]

57. Moreover, of the 1,802 data breaches in 2022, ITRC reported that 1,560 involved compromised names, and 1,143 involved compromised of Social Security Numbers, —types of Private Information included in the unauthorized disclosure in this Data Breach.[29]

58. The risks of cyberattacks are widely known to the public and to anyone in Defendant's industry. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[30]

59. Furthermore, Defendant was aware of the risk of data breaches because such breaches have dominated the headlines in recent years.

60. Private Information is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used for a variety of unlawful and nefarious purposes, including ransomware and fraudulent misuse, and sale on the Dark Web.

61. Private Information can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.

---

[27] Identity Theft Resource Center, 2022 Data Breach Report, available at https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf, pg. 7 (last acc. Jul. 3, 2023).
[28] *See Id*., pg. 2.
[29] *Id*., pg. 6.
[30] IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at https://www.ibm.com/reports/data-breach (last acc. Apr. 14, 2023).

62. Given the nature of the Data Breach, it was foreseeable that the compromised Private Information could be used by hackers and cybercriminals in a variety of different injurious ways. Indeed, the cybercriminals who possess the Class Members' Private Information can easily obtain Class Members' tax returns or open fraudulent credit card accounts in the Class Members' names.

D. Defendant Failed to Comply with FTC Guidelines

63. 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.

64. In 2016, the FTC updated its publication, *Protecting Private Information: A Guide for Business*, which establishes cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of Private 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 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.[31]

65. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require

[31] *See* Federal Trade Commission, October 2016, "Protecting Private information: A Guide for Business," available at https://www.bulkorder.ftc.gov/system/files/publications/2_9-00006_716a_protectingpersinfo-508.pdf (last acc. Apr. 14, 2023).

complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[32]

66. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

67. These FTC enforcement actions include actions against entities failing to safeguard Private Information such as Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 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.").

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

69. Defendant was at all times fully aware of its obligations to protect the Private Information of its current and former employees. Defendant was also aware of the significant repercussions that would result from their failure to do so.

[32] *See id*.

E. Defendant Fails to Comply with Industry Standards

70. As shown above, experts studying cyber security routinely identify organizations holding Private Information as being particularly vulnerable to cyber-attacks because of the value of the information they collect and maintain. As of 2022, ransomware breaches like that which occurred here had grown by 41% in the last year and cost on average $4.54 million dollars.[33]

71. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards. The Center for Internet Security's (CIS) CIS Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including 18 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.[34]

72. In addition, the National Institute of Standards and Technology (NIST) recommends certain practices to safeguard systems, *infra,* such as:

- Control who logs on to your network and uses your computers and other devices.
- Use security software to protect data.

[33] IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at https://www.ibm.com/reports/data-breach (last acc. Apr. 14, 2023).
[34] *See* https://www.rapid7.com/solutions/compliance/critical-controls/ (last acc. Apr. 14, 2023).

- Encrypt sensitive data, at rest and in transit.
- Conduct regular backups of data.
- Update security software regularly, automating those updates if possible.
- Have formal policies for safely disposing of electronic files and old devices.
- 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.[35]

73. Upon information and belief, Defendant failed to meet the minimum standards of both the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and other industry standards for protecting Plaintiff's and the proposed Class Members' Private Information—resulting in the Data Breach.

F. The Data Breach Caused Plaintiff and the Class Members Injury and Damages

74. Plaintiff and members of the proposed Class have suffered injury and damages from the unauthorized disclosure of their Private Information in the Data Breach that can be directly traced to Revance's failures to adequately protect that Private Information, that have occurred, are ongoing, and imminently will occur.

75. As stated prior, in the Data Breach, unauthorized cybercriminals were able to access the Plaintiff's and the proposed Class Members' Private Information, which on information and belief is now being used or will imminently be used for fraudulent purposes and/or has been sold

[35] Understanding The NIST Cybersecurity Framework, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework (last acc. Apr. 14, 2023).

for such purposes and posted on the dark web for sale, causing widespread injury and damages.

76. The ramifications of Defendant's failure to keep Plaintiff's and the Class's Private Information secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, or other information, such as addresses, without permission, to commit fraud or other crimes.

77. As a direct and proximate result of the Data Breach permitted by Defendant to occur, Plaintiff and the Class Members have suffered, will imminently suffer, and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiff and the Class Members have suffered, are at an increased risk of suffering, or will imminently suffer:

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

b. The diminution in value of their Private Information;

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

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

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

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Private Information; and

h. The continued risk to their Private Information, which remains in the

possession of Defendant and is subject to further breaches so long as Revance fails to undertake the appropriate measures to protect the Private Information in its possession.

78. Furthermore, the Data Breach has placed Plaintiff and the proposed Class Members at an increased risk of fraud and identity theft.

79. There are myriad dangers which affect victims of identity theft, including: cybercriminals opening new financial accounts, credit cards, and loans in victim's names; victim's losing health care benefits (medical identity theft); hackers taking over email and other accounts; time and effort to repair credit scores; losing home due to mortgage and deed fraud; theft of tax refunds; hackers posting embarrassing posts on victim's social media accounts; victims spending large amounts of time and money to recover their identities; experiencing psychological harm and emotional distress; victims becoming further victimized by repeat instances of identity theft and fraud; cybercriminals committing crimes in victim's names; victims' personal data circulating the Dark Web forever; victims receiving increased spam telephone calls and emails; victims' children or elderly parents having their identities stolen.[36]

94. The FTC recommends that identity theft victims take several costly steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, seeking a credit freeze, and correcting their credit reports.[37]

---

[36] *See* Gaetano DiNardi, Aura.com, "How Bad Is Identity Theft? Is It Serious?" (December 14, 2022) available at https://www.aura.com/learn/dangers-of-identity-theft#:~:text=Fraudsters%20can%20open%20new%20accounts,to%20repair%20your%20credit%20score (last acc. Feb. 27, 2023).

[37] *See* https://www.identitytheft.gov/Steps (last visited September 1, 2021).

95. The time-consuming process recommended by the FTC and other experts is complicated by the vulnerable situations of Defendant's employees.

96. Identity thieves use stolen Private Information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

97. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

98. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's Private Information to police during an arrest—resulting in an arrest warrant being issued in the victim's name. That can be even more problematic and difficult to remedy for someone who already has a criminal record.

99. Further, according to the Identity Theft Resource Center's 2021 Consumer Aftermath Report, identity theft victims suffer "staggering" emotional tolls: For example, nearly 30% of victims have been the victim of a previous identity crime; an all-time high number of victims say they have contemplated suicide. Thirty-three percent reported not having enough money to pay for food and utilities, while 14% were evicted because they couldn't pay rent or their mortgage. Fifty-four percent reported feelings of being violated. [38]

100. What's more, theft of Private Information is also gravely serious outside of the

[38] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (June 11, 2021), avail. at https://www.creditcards.com/statistics/credit-card-security-id-theft-fraud-statistics-1276/ citing Identity Theft Resource Center, "2021 Consumer Aftermath Report," May 26, 2021 available at https://www.idtheftcenter.org/post/the-identity-theft-resource-centers-2021-consumer-aftermath-report-reveals-impacts-on-covid-19-identity-crime-victims/ (last acc. Feb. 27, 2023).

traditional risks of identity theft. In the last two decades, as more and more of our lives become interconnected through the lens of massively complex cloud computing, Private Information is a valuable property right.[39]

102. The value of sensitive information is axiomatic; one need only consider the value of Big Data in corporate America, or that the consequences of cyber theft include heavy prison sentences. Even the obvious risk to reward analysis of cybercrime illustrates beyond doubt that Private Information has considerable market value.

103. Theft of Private Information, in particular, is problematic because: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[40]

104. It must also be noted there may be a substantial time lag–measured in years–between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

105. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

106. Where the most Private Information belonging to Plaintiff and Class Members was accessible from Defendant's network, there is a strong probability that entire batches of stolen

---

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

[40] *See Medical Identity Theft, Federal Trade Commission Consumer Information* (last visited: June 7, 2022), http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and the Class Members are at an increased risk of fraud and identity theft for many years into the future.

107. Thus, Plaintiff and the Class Members must vigilantly monitor their financial and medical accounts for many years to come.

108. Social Security numbers are among the worst kind of Private Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.[41]

109. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[42] Each of these fraudulent activities is difficult to detect. An individual may not know that her or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

110. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he

[41] *See* U.S. Social Security Administration, "Identity Theft and Your Social Security Number," Publication No. 05-10064, July 2021, available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last acc. Feb. 25, 2023)
[42] *See id.*

credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[43]

111. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[44] Medical information is especially valuable to identity thieves. The asking price on the Dark Web for medical data is $50 per person and up.[45]

112. Accordingly, the Data Breach has caused Plaintiff and the proposed Class Members a greatly increased risk of identity theft and fraud, in addition to the other injuries and damages set forth herein, specifically the imminent identity fraud and criminal fraudulent activity; lost time and efforts in remediating the impact of the Data Breach, and other injury and damages as set forth in the preceding paragraphs.

113. Defendant knew or should have known of these harms which would be caused by the Data Breach it permitted to occur, and strengthened its data systems accordingly.

CLASS ALLEGATIONS

116. Plaintiff sues on behalf of herself and the proposed Class, defined as follows:

> **All persons whose Private Information was compromised in the Data Breach experienced by Revance beginning on or about March 15, 2023, as announced by Defendant in July 2023.**

---

[43] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited September 1, 2021).

[44] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited September 1, 2021).

[45] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/ (last accessed September 1, 2021).

117. The following people are excluded from the Class: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's members, partners, subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or its parents has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

118. The Class defined above is identifiable through Defendant's business records.

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

120. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Tenn. R. Civ. P. 23.01(1)-(4):

a. Numerosity. Plaintiff is representative of the proposed Class, consisting of approximately 2,803 individuals, which are identifiable based on Defendant's records, and far too many to join in a single action;

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

c. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's interests. Plaintiff's interests do not conflict with Class Members' interests and Plaintiff has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel. Defendant has no defenses unique to Plaintiff.

d. Commonality. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Common questions for the Class include, but are not necessarily limited to the following:

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

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

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

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

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

vi. Whether Defendant's Data Breach Notice was reasonable;

vii. Whether Defendant's conduct was likely to deceive the public;

viii. Whether Defendant is liable for negligence;

ix. Whether Defendant was negligent *per se*;

x. Whether Defendant's practices and representations related to the Data Breach breached implied contracts;

xi. Whether Defendant was unjustly enriched;

xii. Whether the Data Breach caused Plaintiff and the Class injuries and damages;

xiii. What the proper damages measure is; and

xiv. Whether Plaintiff and the Class are entitled to damages, or declaratory and injunctive relief.

121. Further, this action satisfies Tenn. R. Civ. P. 23.02 because: (i) common questions of law and fact predominate over any individualized questions; (ii) prosecuting individual actions would create a risk of inconsistent or varying adjudications, risking incompatible standards of conduct for Defendant, and a risk adjudications with respect to individual members of the Class which would as a practical matter be dispositive of the interests of the other members not parties to the adjudications or would substantially impair or impede their ability to protect their interest; and (iii) the Defendant have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

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

122. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

123. Plaintiff and the Class Members entrusted their Private Information to Revance as a condition of employment.

124. Defendant owed to Plaintiff and Class Members a duty to exercise reasonable care in handling and using the Private Information in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

125. Defendant owed a duty of care to Plaintiff and Class Members because it was

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

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

127. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and members of the Class's Private Information as a condition of employment.

128. The risk that unauthorized persons would attempt to gain access to the Private Information, and misuse it, was foreseeable. Given that Defendant holds vast amounts of Private Information, it was inevitable that unauthorized individuals would attempt to access Defendant's

databases containing the Private Information—whether by a sophisticated cyberattack or otherwise.

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

130. Defendant breached its duties by failing to exercise reasonable care in supervising its agents and in handling and securing the Private Information of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff's and Class Members' injuries.

131. Defendant further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and Class Members' injuries-in-fact.

132. As a direct, proximate, and traceable result of Defendant's negligence, Plaintiff and the Class Members have suffered or will imminently suffer damages, as set forth in the preceding paragraphs.

133. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused and will imminently cause Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, misuse of Private Information, lost time and effort spent mitigating the effects of the Data Breach, feeling of anxiety, emotional distress, loss of the opportunity to control how their Private Information is used, diminution in value of their Private Information; the compromise and continuing publication of their Private Information; out-of-pocket costs associated with the prevention, detection, recovery,

and remediation from identity theft or fraud; Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach; delay in receipt of tax refund monies; unauthorized use of stolen Private Information; and increased risk of harm. Said injury-in-fact and damages are ongoing, imminent, immediate, and which Plaintiff and the Class Members continue to face.

134. Further, Plaintiff and the Class are entitled to injunctive relief ordering Defendant to strengthen its data security systems, monitoring procedures, and data breach notification procedures to prevent additional unauthorized disclosure of the Private Information in Defendant's possession.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

135. Plaintiff incorporates the above Paragraphs as if fully set forth herein.

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

137. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, employees' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the members of the Class's sensitive PII.

138. Defendant violated its duties under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's Private Information and not complying with applicable industry standards as described in detail herein. Defendant's conduct was

particularly unreasonable given the nature and amount of Private Information Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to employees in the event of a breach, which ultimately came to pass.

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

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

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

142. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

143. But-for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

144. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

145. Had Plaintiff and members of the Class known that Defendant did not adequately

protect their Private Information, Plaintiff and members of the Class would not have entrusted Defendant with their Private Information.

146. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members suffered actual, tangible, injury-in-fact and damages, including, misuse of Private Information, lost time and effort spent mitigating the effects of the Data Breach, feeling of anxiety, emotional distress, loss of the opportunity to control how their Private Information is used, diminution in value of their Private Information; the compromise and continuing publication of their Private Information; out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud; Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach; delay in receipt of tax refund monies; unauthorized use of stolen Private Information; and increased risk of harm. Said injury-in-fact and damages are ongoing, imminent, immediate, and which Plaintiff and the Class Members continue to face.

COUNT III
BREACH OF AN IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

147. Plaintiff incorporates the above Paragraphs as if fully set forth herein.

148. Defendant offered to provide employment to Plaintiff and the Class Members in exchange for their labor and Private Information.

149. In turn, and through internal policies described in the preceding paragraphs, and other conduct and representations, Revance agreed it would not disclose the Private Information it collects to unauthorized persons and that it would safeguard employee Private Information.

150. Plaintiff and the Class Members accepted Revance's offer by providing Private Information to Defendant and rendering labor to Defendant.

151. Implicit in the parties' agreement was that Revance would adequately safeguard the Private Information of Plaintiff and the Class Members and would provide them with prompt and adequate notice of all unauthorized access and/or theft of their Private Information.

152. Plaintiff and the Class Members would not have entrusted their Private Information to Revance in the absence of such an agreement with Revance.

153. Revance materially breached the contract(s) it had entered into with Plaintiff and the Class Members by failing to safeguard their Private Information, and by failing to notify them promptly of the Data Breach that compromised such information. Revance further breached the implied contracts with Plaintiff and the Class Members by:

a. Failing to properly safeguard and protect Plaintiff's and members of the Class's Private Information;

b. Failing to comply with industry standards, as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to properly supervise its agents in possession of Private information;

d. Failing to ensure the confidentiality and integrity of electronic Private Information that Defendant created, received, maintained, and transmitted.

154. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Revance's material breaches of its agreement(s).

155. Plaintiff and the Class Members have performed as required under the relevant agreements, or such performance was waived by the conduct of Revance.

156. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in

connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

157. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

158. Revance failed to advise Plaintiff and members of the Class of the Data Breach promptly and sufficiently.

159. In these and other ways, Revance violated its duty of good faith and fair dealing.

160. Plaintiff and the Class Members have sustained injury-in-fact and damages because of Revance's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

161. Plaintiff incorporates the above Paragraphs 1-121 if fully set forth herein.

162. This claim is pleaded as the alternative to the breach of implied contractual duty claim.

163. Plaintiff and the Class Members conferred a benefit upon Defendant in the form of labor rendered to Defendant in connection with employment, and by providing their Private Information to Defendant as a condition of employment.

164. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and the Class Members.

165. As a result of Defendant's conduct, Plaintiff and members of the Class suffered actual damages in an amount equal to the difference in value between the value of their labor with reasonable data privacy and security practices and procedures, and the value of labor without unreasonable data privacy and security practices and procedures that they received.

166. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the proposed Class Members' labor and their Private Information because Defendant failed to adequately protect their Private Information. Plaintiff and the Class Members would not have provided their Private Information, nor rendered labor to Defendant, had they known Defendant would not adequately protect their Private Information.

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

COUNT V
INVASION OF PRIVACY—PUBLIC DISCLOSURE OF PRIVATE FACTS
(On Behalf of Plaintiff and the Class)

168. Plaintiff incorporates the above Paragraphs as if fully set forth herein.

169. The Plaintiff and the Class Members took reasonable and appropriate steps to keep their Private Information confidential from the public.

170. Plaintiff's and the Class Members' efforts to safeguard their own Private Information were successful, as their Private Information was not known to the general public prior to the Data Breach.

171. Plaintiff and the Class Members had a legitimate expectation of privacy to their Private Information, entrusted solely to Revance for purpose of employment, and were entitled to the protection of this information against disclosure to unauthorized third parties.

172. Defendant owed a duty to Revance's employees, including Plaintiff and the Class Members, to keep their Private Information confidential.

173. The unauthorized release of Private Information by Defendant in the Data Breach is highly offensive to a reasonable person.

174. Plaintiff's and the Class Members' Private Information is not of legitimate concern to the public.

175. Defendant knew or should have known that Plaintiff's and Class Members' Private Information was private, confidential, and should not be disclosed.

176. Defendant publicized Plaintiff's and members of the Class's Private Information, by unauthorizedly disclosing it to cyber criminals who had no legitimate interest in this Private Information and who had the express purpose of monetizing that information through fraudulent misuse and by injecting it into the illicit stream of commerce flowing through the Dark Web.

177. Indeed, not only is Plaintiff's and members of the Class's Private Information published on the Dark Web, upon information and belief, but is being used to commit fraud; it is being disseminated amongst, *inter alia,* other criminals, financial institutions, merchants, creditors, health care providers and governmental agencies.

178. It is therefore substantially certain that the Plaintiff's and the Class Members' Private Information is rapidly becoming public knowledge—among the community at large—due to the nature of the cyber-attack that procured it, and the identity theft for which it is designed.

179. As a direct and proximate result of the invasion of privacy, public disclosure of private facts committed by Defendant, Plaintiff and the members of the Class have suffered injury-in-fact and damages as set forth in the preceding paragraphs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, KAREN LYTLE, individually, and on behalf of all others similarly situated, requests that the Court enter an order:

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

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

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

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

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

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

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

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

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

JURY DEMAND

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

Dated: August 15, 2023 Respectfully submitted,

/s/ J. Gerard Stranch, IV
J. Gerard Stranch, IV (No. 23045)
Andrew E. Mize (*Pro Hac Vice* forthcoming)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
amize@stranchlaw.com

Samuel Strauss (*Pro Hac Vice* forthcoming)
Raina Borelli (*Pro Hac Vice* forthcoming)
TURKE & STRAUSS, LLP
613 Williamson Street Suite 201
Madison, WI 53703
(608) 237-1775
Sam@turkestrauss.com
raina@turkestrauss.com

Counsel for Plaintiff and the Proposed Class