SALTZ MONGELUZZI & BENDESKY P.C.
BY: Patrick Howard, Esq.
Identification No: 88572
1650 Market Street, 52nd Floor
Philadelphia, PA 19103
(215) 496-8282

TURKE & STRAUSS LLP
Samuel J. Strauss*
Raina Borrelli*
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
(608) 237-1775
**to be admitted pro hac vice*

Attorneys for Plaintiff and the Proposed Class

STEVEN BOWER, on behalf of himself and all others similarly situated,

Plaintiff,

v.

BRODART CO.,

Defendant.

PHILADELPHIA COUNTY COURT OF COMMON PLEAS

FEBRUARY TERM, 2024
No.

CLASS ACTION COMPLAINT IN A CIVIL ACTION

JURY TRIAL DEMANDED

"NOTICE"

"You have been sued in court. If you wish to defend against the claims set forth in the following pages, you must take action within twenty (20) days after this complaint and notice are served, by entering a written appearance personally or by an attorney and filing in writing with the court your defenses or objections to the claims set forth against you. You are warned that if you fail to do so the case may proceed without you and a judgement may be entered against you by the court without further notice for any money claimed in the complaint or for any other claim or relief requested by the plaintiff. You may lose money or property or other rights important to you.

"YOU SHOULD TAKE THIS PAPER TO YOUR LAWYER AT ONCE. IF YOU DO NOT HAVE A LAWYER OR CANNOT AFFORD ONE, GO TO OR TELEPHONE THE OFFICE SET FORTH BELOW TO FIND OUT WHERE YOU CAN GET LEGAL HELP.

THIS OFFICE CAN PROVIDE YOU WITH INFORMATION ABOUT HIRING A LAWYER.
IF YOU CANNOT AFFORD TO HIRE A LAWYER, THIS OFFICE MAY BE ABLE TO PROVIDE YOU WITH INFORMATION ABOUT AGENCIES THAT MAY OFFER LEGAL SERVICES TO ELIGIBLE PERSONS AT A REDUCED FEE OR NO FEE.

PHILADELPHIA BAR ASSOCIATION
LAWYER REFERRAL and INFORMATION SERVICE
One Reading Center
Philadelphia, Pennsylvania 19107
(215) 238-1701"

"AVISO

"Le han demandado en corte. Si usted quiere defenderse contra las demandas nombradas en las páginas siguientes, tiene veinte (20) días, a partir de recibir esta demanda y la notificación para entablar personalmente o por un abogado una comparecencia escrita y tambien para entablar con la corte en forma escrita sus defensas y objeciones a las demandas contra usted. Sea avisado que si usted no se defiende, el caso puede continuar sin usted y la corte puede incorporar un juicio contra usted sin previo aviso para conseguir el dinero demandado en el pleito o para conseguir cualquier otra demanda o alivio solicitados por el demandante. Usted puede perder dinero o propiedad u otros derechos importantes para usted.

USTED DEBE LLEVAR ESTE DOCUMENTO A SU ABOGADO INMEDIATAMENTE. SI USTED NO TIENE ABOGADO (O NO TIENE DINERO SUFICIENTE PARA PARGAR A UN ABOGADO), VAYA EN PERSONA O LLAME POR TELEFONO LA OFICINA NOMBRADA ABAJO PARA AVERIGUAR DONDE SE PUEDE CONSEGUIR ASSISTENCIA LEGAL. ESTA OFICINA PUEDE PROPORCIONARLE LA INFORMACION SOBRE CONTRATAR A UN ABOGADO.

SI USTED NO TIENE DINERO SUFICIENTE PARA PAGAR A UN ABOGADO, ESTA OFICINA PUEDE PROPORCIONARLE INFORMACION SOBRE AGENCIAS QUE OFRECEN SERVICIOS LEGALES A PERSONAS QUE CUMPLEN LOS REQUISITOS PARA UN HONORARIO REDUCIDO O NINGUN HONORARIO.

ASSOCIACION DE LICENDIADOS DE FILADELFIA
SERVICO DE REFERENCA E INFORMACION LEGAL
One Reading Center,
Filadelfia, Pennsylvania 19107
Telefono: (215) 238-1701"

Steven Bower ("Plaintiff"), through his attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Brodart Co. ("Brodart" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiff alleges the following on information and belief—except as to his own actions, counsel's investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Defendant's failure to protect highly sensitive data.

2. Defendant is a company that sells various products and services to libraries across Pennsylvania and nationwide.[1]

3. As such, Defendant stores a litany of highly sensitive personal identifiable information ("PII") and protected health information ("PHI")—together "PII/PHI"—about its current and former employees (and the former employees of Brodart's past affiliates). But Defendant lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the "Data Breach").

4. It is unknown for precisely how long the cybercriminals had access to Defendant's network before the breach was discovered. In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to the PII/PHI of Defendant's current and former employees (and the former employees of Brodart's past affiliates).

[1] *Notification of Data Breach*, MAINE ATTY GEN, https://apps.web.maine.gov/online/aeviewer/ME/40/68039b86-a480-4cfb-bf25-13e85219c72b.shtml (last visited Feb. 26, 2024).

5. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's PII/PHI. In short, Defendant's failures placed the Class's PII/PHI in a vulnerable position—rendering them easy targets for cybercriminals.

6. Plaintiff is a Data Breach victim, having received a breach notice—attached as Exhibit A. He brings this class action on behalf of himself, and all others harmed by Defendant's misconduct.

7. The exposure of one's PII/PHI to cybercriminals is a bell that cannot be unrung. Before this data breach, its current and former employees' private information was exactly that—private. Not anymore. Now, their private information is forever exposed and unsecure.

PARTIES

8. Plaintiff, Steven Bower, is a natural person and citizen of Pennsylvania. He resides in Williamsport, Pennsylvania where he intends to remain.

9. Defendant, Brodart Co., is a Domestic General Partnership incorporated in Pennsylvania and with its principal place of business at 500 Arch Street, Williamsport, Pennsylvania 17701.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action under 42 Pa. Cons. Stat. § 931.

11. This Court has personal jurisdiction over Defendant because it is headquartered in Pennsylvania, regularly conducts business in Pennsylvania, and has sufficient minimum contacts in Pennsylvania.

12. Venue is proper under 231 Pa. Code § 2179 because Defendant regularly conducts business in Philadelphia county.

BACKGROUND

Defendant Collected and Stored the PII/PHI of Plaintiff and the Class

13. Defendant is a company that sells various products and services to libraries across Pennsylvania and nationwide.[2]

14. As part of its business, Defendant receives and maintains the PII/PHI of thousands of its current and former employees (and the former employees of Brodart's past affiliates).

15. 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, Plaintiff and Class members themselves took reasonable steps to secure their PII/PHI.

16. Under state and federal law, businesses like Defendant have duties to protect the PII/PHI of Defendant's current and former employees (and the former employees of Brodart's past affiliates) and to notify them about breaches.

17. Defendant recognizes these duties, declaring that in its "Privacy Policy" that:

a. "We will not share the personal information you provide except . . . with your consent[.]"[3]

---

[2] *Notification of Data Breach*, MAINE ATTY GEN, https://apps.web.maine.gov/online/aeviewer/ME/40/68039b86-a480-4cfb-bf25-13e85219c72b.shtml (last visited Feb. 26, 2024).

[3] *Privacy Policy*, BRODART, https://www.shopbrodart.com/Privacy_Policy (last visited Feb. 26, 2024).

b. "This notice explains our online information collection and use practices and the choices you can make about the way we use and share such information."[4]

c. "We do not consider any companies that are within our 'family' of companies to be 'third parties' for purposes of this policy. . . . However, if we pass on personal information to a family company, we require that it protect such information in a manner that is consistent with this policy."[5]

d. "We believe we have in place the appropriate physical, electronic, and managerial procedures to safeguard and help prevent unauthorized access, maintain data security and correctly use the information we collect online as well as offline."[6]

e. "When your personal information is passed onto non-affiliated companies, to the extent practical, we require that they also have in place the appropriate safeguards."[7]

Defendant's Data Breach

18. On or before October 14, 2023, Defendant was hacked—and "began experiencing an outage of our websites and our server-based IT and business."[8]

19. Worryingly, Defendant already admitted that "we have since confirmed the outage was the result of a malware-related data security attack by unauthorized third parties."[9]

---

[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *Id.*

20. And Defendant admitted that, even after the Data Breach began, it was unable to prevent further injury due to its Data Breach—including the ***publishing*** of PII/PHI by cybercriminals on the Dark Web.[10] Specifically, Defendant explained that:

a. "Unfortunately, despite our efforts, we have been unable to prevent the risk of further disclosure of the inappropriately accessed data."[11]

b. "On October 31, 2023, we were notified that a portion of the data had been disclosed on the internet by the unauthorized third parties."[12]

c. "On November 1, 2023, we learned that some personal information of employees was included within the data accessed and disclosed by the unauthorized third parties."[13]

21. Because of Defendant's Data Breach, at least the following types of PII/PHI were compromised:

a. names;

b. addresses;

c. Social Security numbers;

d. dates of birth;

e. driver's license numbers;

f. medical information;

g. financial information;

h. financial account numbers and passwords;

---

[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *Id.*

i. credit card numbers (in combination with security code, access code, password or PIN for the account); and

j. debit card numbers (in combination with security code, access code, password or PIN for the account).[14]

22. In total, Defendant injured at least 8,259 persons—via the exposure of their PII/PHI—in the Data Breach. Upon information and belief, these 8,259 persons include its current and former employees (and the former employees of Brodart's past affiliates).

23. Beyond its current and former employees, Defendant also indicates that its Data Breach injured the former employees of "our former affiliate companies (Tura, CRS, J.K. Gill, or Stacey's)."[15]

24. And yet, Defendant waited over until November 22, 2023 before it began notifying the class—a full 39 days after the Data Breach was discovered.[16]

25. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

26. And when Defendant did notify Plaintiff and the Class of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiff and the Class:

a. "We recommend that you review your credit card and bank information, including your statements and charges."[17]

---

[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Id.*

b. "Please also review the attachments to this letter, titled Steps You Can Take to Help Protect Your Information, and How to Enroll in Credit Monitoring and Identity Theft Protection Services for further information."[18]

c. "[W]e recommend that you remain vigilant by reviewing your account statements and credit reports closely."[19]

d. "[R]eport any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC)."[20]

e. "You may want to consider placing a fraud alert on your credit report."[21]

f. "[C]ontact [your] Attorney General for more information and assistance."[22]

27. Defendant failed its duties when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII/PHI. And thus, Defendant caused widespread injury and monetary damages.

28. Since the breach, Defendant has "implement[ed] additional best-in-class tools to further fortify our overall security posture, including enhancing our anti-intrusion measures and anti-virus protection tools."[23]

29. But this is too little too late. Simply put, these measures—which Defendant now recognizes as necessary—should have been implemented *before* the Data Breach.

---

[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *Id.*

30. On information and belief, Defendant failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

31. Further, the Notice of Data Breach shows that Defendant cannot—or will not—determine the full scope of the Data Breach, as Defendant has been unable to determine precisely what information was stolen and when.

32. Defendant has done little to remedy its Data Breach. True, Defendant has offered some victims credit monitoring and identity related services. But upon information and belief, such services are wholly insufficient to compensate Plaintiff and Class members for the injuries that Defendant inflicted upon them.

33. Because of Defendant's Data Breach, the sensitive PII/PHI of Plaintiff and Class members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class members.

34. Worryingly, the cybercriminals that obtained Plaintiff's and Class members' PII/PHI appear to be the notorious "Playcrypt" group.[24]

35. Playcrypt (a.k.a., "Play Ransomware") is an especially notorious cybercriminal group. In fact, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) released a joint report warning the public about Play Ransomware.[25]Specifically, the joint "Cybersecurity Advisory" (CSA) stated, *inter alia*, that:

---

[24] *See e.g., Play*, RANSOMLOOK (Oct. 10, 2023) https://www.ransomlook.io/group/play; *Play Ransomware Victim: Brodart*, REDPACKET SECURITY (Oct. 31, 2023), https://www.redpacketsecurity.com/play-ransomware-victim-brodart/.
[25] *#StopRansomware: Play Ransomware*, FBI & CISA (Dec. 18, 2023) https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a.

a. "Since June 2022, the Play (also known as Playcrypt) ransomware group has impacted a wide range of businesses and critical infrastructure in North America, South America, and Europe."[26]

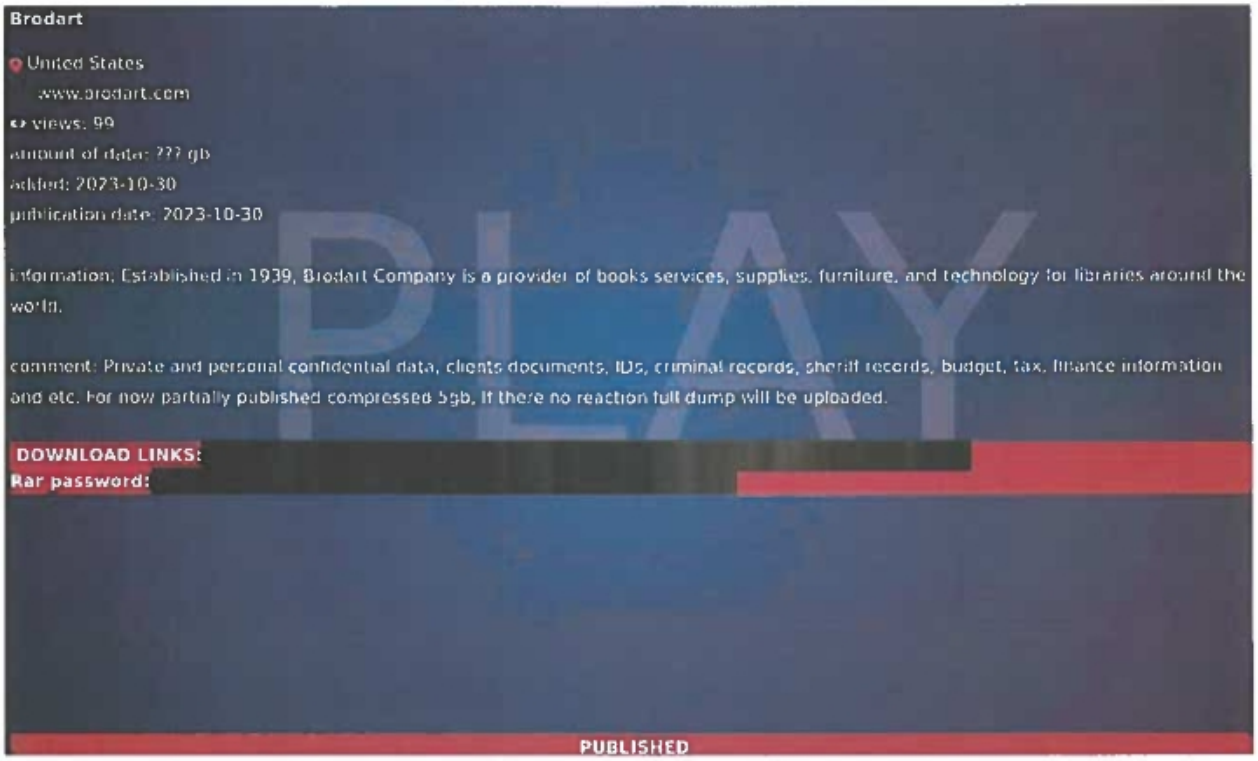
b. "The Play ransomware group is presumed to be a closed group, designed to 'guarantee the secrecy of deals,' according to a statement on the group's data leak website."[27]

c. "Play ransomware actors employ a double-extortion model, encrypting systems after exfiltrating data."[28]

d. "If a victim refuses to pay the ransom demand, the ransomware actors threaten to publish exfiltrated data to their leak site on the Tor network."[29]

36. Worryingly, a screenshot of Playcrypt's website on the Dark Web appears to confirm that the stolen PII/PHI was ***already published***.[30]

[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.*
[30] *Play*, RANSOMLOOK (Oct. 10, 2023) https://www.ransomlook.io/group/play.



37. Specifically, the Dark Web site reveals that:

a. Playcrypt possesses "[p]rivate and personal confidential data, client documents, IDs, criminal records, sheriff records, budget, tax, finance information and etc."[31]

b. Playcrypt will publish the "full dump" if "there is no reaction."[32]

c. And Playcrypt *already published* a "compressed 5gb" of PII/PHI—specifically providing (1) a download link, and (2) a password to access that data.[33]

[31] *Id.*
[32] *Id.*
[33] *Id.* For the privacy of the Data Breach victims, counsel has redacted the link and password from the screenshot.

38. And as the Harvard Business Review notes, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[34]

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

Plaintiff's Experiences and Injuries

40. Plaintiff Steven Bower is a former employee of Defendant—having worked for Defendant for approximately one year in 2005, and for approximately one week in 2017.

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

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

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

44. Plaintiff 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's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

45. Plaintiff reasonably understood that a portion of the funds derived from his employment would be used to pay for adequate cybersecurity and protection of PII/PHI.

---

[34] Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back.

46. Plaintiff does not recall ever learning that his information was compromised in a data breach incident—other than the breach at issue here.

47. Plaintiff received a Notice of Data Breach dated November 22, 2023—attached as Exhibit A.

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

49. Through its Data Breach, Defendant compromised Plaintiff's:

a. name;

b. address;

c. Social Security number;

d. date of birth;

e. driver's license number;

f. medical information;

g. financial information;

h. financial account numbers and passwords;

i. credit card number (in combination with security code, access code, password or PIN for the account); and

j. debit card number (in combination with security code, access code, password or PIN for the account).

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

51. And in the aftermath of the Data Breach, Plaintiff has suffered from a spike in spam and scam emails, text messages and phone calls (including scams whereby the sender purports to be from Verizon).

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

53. Because of Defendant's Data Breach, Plaintiff 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's injuries are precisely the type of injuries that the law contemplates and addresses.

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

55. Plaintiff 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.

56. Plaintiff 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.

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

58. Today, Plaintiff 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 and the Proposed Class Face Significant Risk of Continued Identity Theft

59. Because of Defendant's failure to prevent the Data Breach, Plaintiff and Class members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their PII/PHI is used;

b. diminution in value of their PII/PHI;

c. compromise and continuing publication of their PII/PHI;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII/PHI; and

h. continued risk to their PII/PHI—which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the PII/PHI.

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

61. The value of Plaintiff and Class's PII/PHI on the black market is considerable. Stolen PII/PHI trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "Dark Web"—further exposing the information.

62. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII/PHI far and wide.

63. One way that criminals profit from stolen PII/PHI is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen PII/PHI, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

64. The development of "Fullz" packages means that the PII/PHI exposed in the Data Breach can easily be linked to data of Plaintiff and the Class that is available on the internet.

65. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII/PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and Class members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class members' stolen PII/PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

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

67. Defendant's failure to promptly and properly notify Plaintiff and Class members of the Data Breach exacerbated Plaintiff and Class members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII/PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant Knew—Or Should Have Known—of the Risk of a Data Breach

68. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

69. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.[35]

70. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[36]

71. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant Failed to Follow FTC Guidelines

72. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines

---

[35] *See 2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) https://notified.idtheftcenter.org/s/.

[36] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

73. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[37] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

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

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

74. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

75. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

76. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and

[37] *Protecting Personal Information: A Guide for Business*. FEDERAL TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

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.

77. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to the PII/PHI of Defendant's current and former employees (and the former employees of Brodart's past affiliates) constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

78. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

79. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

80. Defendant failed to meet the minimum standards of any of the following frameworks: 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 all established standards in reasonable cybersecurity readiness.

81. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

Defendant Violated HIPAA

82. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[38]

83. 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.[39]

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

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

---

[38] 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.

[39] *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).

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

c. 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 C.F.R. § 164.306(a)(3);

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

e. failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

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

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

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

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

85. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

CLASS ACTION ALLEGATIONS

86. Plaintiff brings this class action under Pa. R. Civ. P. 1701, individually and on behalf of all members of the following class:

> All individuals residing in Pennsylvania whose PII/PHI was compromised in the Data Breach discovered by Brodart in October 2023, including all those individuals who received notice of the breach.

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

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

89. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

90. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some individuals and sent them data breach notices.

91. Numerosity. The Class members are so numerous that joinder of all Class members is impracticable. Upon information and belief, the proposed Class includes at least 8,259 members.

92. Typicality. Plaintiff's claims are typical of Class members' 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.

93. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's common interests. His interests do not conflict with Class members' interests. And Plaintiff has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

94. Commonality and Predominance. Plaintiff's and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class members—for which a class wide proceeding can answer for all Class members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII/PHI;

b. if 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;

c. if Defendant were negligent in maintaining, protecting, and securing PII/PHI;

d. if Defendant breached contract promises to safeguard Plaintiff and the Class's PII/PHI;

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

f. if Defendant's Breach Notice was reasonable;

g. if the Data Breach caused Plaintiff and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiff and the Class are entitled to damages, treble damages, and or injunctive relief.

95. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

96. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

97. Plaintiff and the Class (or their third-party agents) entrusted their PII/PHI to Defendant on the premise and with the understanding that Defendant would safeguard their PII/PHI, use their PII/PHI for business purposes only, and/or not disclose their PII/PHI to unauthorized third parties.

98. Defendant owed a duty of care to Plaintiff and Class members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII/PHI in a data breach. And here, that foreseeable danger came to pass.

99. Defendant has full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiff and the Class could and would suffer if their PII/PHI was wrongfully disclosed.

100. Defendant owed these duties to Plaintiff and Class members 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 practices. After all, Defendant actively sought and obtained Plaintiff and Class members' PII/PHI.

101. Defendant owed—to Plaintiff and Class members—at least the following duties to:

a. exercise reasonable care in handling and using the PII/PHI in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiff and Class members within a reasonable timeframe of any breach to the security of their PII/PHI.

102. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class members to take appropriate measures to protect their PII/PHI, 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.

103. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII/PHI it was no longer required to retain under applicable regulations.

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

105. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class (or their third-party agents) entrusted Defendant with their confidential PII/PHI, a necessary part of obtaining services from Defendant.

106. The risk that unauthorized persons would attempt to gain access to the PII/PHI and misuse it was foreseeable. Given that Defendant hold vast amounts of PII/PHI, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII/PHI —whether by malware or otherwise.

107. PII/PHI is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII/PHI of Plaintiff and Class members' and the importance of exercising reasonable care in handling it.

108. Defendant improperly and inadequately safeguarded the PII/PHI of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

109. Defendant breached these duties as evidenced by the Data Breach.

110. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class members' PII/PHI by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the PII/PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

111. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII/PHI of Plaintiff and Class members which actually and proximately caused the Data Breach and Plaintiff and Class members' injury.

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

113. Defendant has admitted that the PII/PHI of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

114. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

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

116. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII/PHI by criminals, improper disclosure of their PII/PHI, lost benefit of their bargain, lost value of their

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

WHEREFORE, Plaintiff and Class members respectfully request judgment against Defendant and that the Court enter an order:

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

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

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

D. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

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

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 other relief that this Court finds appropriate.

SECOND CAUSE OF ACTION
Negligence *per se*
(On Behalf of Plaintiff and the Class)

117. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

118. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PII/PHI.

119. 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 the PII/PHI entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the Class members' sensitive PII/PHI.

120. Defendant breached its respective duties to Plaintiff and Class members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII/PHI.

121. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII/PHI and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

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

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

124. The injury and harm suffered by Plaintiff and Class members was 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/PHI.

125. Similarly, under HIPAA, Defendant had a duty to follow HIPAA standards for privacy and security practices—as to protect Plaintiff's and Class members' PHI.

126. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect its PHI and by not complying with applicable regulations detailed *supra*. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of PHI that Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

127. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

128. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

WHEREFORE, Plaintiff and Class members respectfully request judgment against Defendant and that the Court enter an order:

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

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

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

D. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

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

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 other relief that this Court finds appropriate.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

129. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

130. Plaintiff and Class members either directly contracted with Defendant or Plaintiff and Class members were the third-party beneficiaries of contracts with Defendant.

131. Plaintiff and Class members (or their third-party agents) were required to provide their PII/PHI to Defendant as a condition of receiving employment provided by Defendant. Plaintiff and Class members (or their third-party agents) provided their PII/PHI to Defendant or its third-party agents in exchange for Defendant's employment.

132. The contracts entered into by Plaintiff's and Class members' agents (for example, their employers), were made for the direct benefit of Plaintiff and the Class.

133. Plaintiff and Class members (or their third-party agents) reasonably understood that a portion of the funds derived from their employment would be used to pay for adequate cybersecurity measures.

134. Plaintiff and Class members (or their third-party agents) reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

135. Plaintiff and the Class members (or their third-party agents) accepted Defendant's offers by disclosing their PII/PHI to Defendant or its third-party agents in exchange for employment.

136. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII/PHI to unauthorized persons.

137. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiff's and Class Member's PII/PHI.

138. Implicit in the parties' agreement was that Defendant would provide Plaintiff and Class members (or their third-party agents) with prompt and adequate notice of all unauthorized access and/or theft of their PII/PHI.

139. After all, Plaintiff and Class members (or their third-party agents) would not have entrusted their PII/PHI to Defendant (or their third-party agents) in the absence of such an agreement with Defendant.

140. Plaintiff and the Class (or their third-party agents) fully performed their obligations under the implied contracts with Defendant.

141. The covenant of good faith and fair dealing is an element of every contract. Thus, 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—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

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

143. Defendant materially breached the contracts it entered with Plaintiff and Class members (or their third-party agents) by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII/PHI that Defendant created, received, maintained, and transmitted.

144. In these and other ways, Defendant violated its duty of good faith and fair dealing.

145. Defendant's material breaches were the direct and proximate cause of Plaintiff's and Class members' injuries (as detailed *supra*).

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

147. Plaintiff and Class members (or their third-party agents) performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

WHEREFORE, Plaintiff and Class members respectfully request judgment against Defendant and that the Court enter an order:

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

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

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

D. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

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

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 other relief that this Court finds appropriate.

FOURTH CAUSE OF ACTION
Invasion of Privacy

(On Behalf of Plaintiff and the Class)

148. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

149. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII/PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

150. Defendant owed a duty to its current and former employees (and the former employees of Brodart's past affiliates), including Plaintiff and the Class, to keep this information confidential.

151. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff and Class members' PII/PHI is highly offensive to a reasonable person.

152. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class (or their third-party agents) disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

153. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

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

155. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

156. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

157. As a proximate result of Defendant's acts and omissions, the private and sensitive PII/PHI of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages (as detailed *supra*).

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

159. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII/PHI are still maintained by Defendant with their inadequate cybersecurity system and policies.

160. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII/PHI of Plaintiff and the Class.

161. In addition to injunctive relief, Plaintiff, on behalf of himself and the other Class members, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

WHEREFORE, Plaintiff and Class members respectfully request judgment against Defendant and that the Court enter an order:

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

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

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

D. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

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

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 other relief that this Court finds appropriate.

FIFTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

162. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

163. This claim is pleaded in the alternative to the breach of implied contract claim.

164. Plaintiff and Class members (or their third-party agents) conferred a benefit upon Defendant. After all, Defendant benefitted from using their PII/PHI and labor to facilitate its business and provision of employment.

165. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class members (or their third-party agents).

166. Plaintiff and Class members (or their third-party agents) reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

167. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class members' PII/PHI.

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

169. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class members' employment and PII/PHI because Defendant failed to adequately protect their PII/PHI.

170. Plaintiff and Class members have no adequate remedy at law.

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

WHEREFORE, Plaintiff and Class members respectfully request judgment against Defendant and that the Court enter an order:

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

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

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

D. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

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

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 other relief that this Court finds appropriate.

SIXTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

172. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

173. Given the relationship between Defendant and Plaintiff and Class members, where Defendant became guardian of Plaintiff's and Class members' PII/PHI, Defendant became a

fiduciary by its undertaking and guardianship of the PII/PHI, to act primarily for Plaintiff and Class members, (1) for the safeguarding of Plaintiff and Class members' PII/PHI; (2) to timely notify Plaintiff and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

174. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their PII/PHI.

175. Because of the highly sensitive nature of the PII/PHI, Plaintiff and Class members (or their third-party agents) would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII/PHI had they known the reality of Defendant's inadequate data security practices.

176. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class members' PII/PHI.

177. Defendant also breached its fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

178. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

WHEREFORE, Plaintiff and Class members respectfully request judgment against Defendant and that the Court enter an order:

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

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

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

D. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

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

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 other relief that this Court finds appropriate.

SEVENTH CAUSE OF ACTION
Breach of Confidence
(On Behalf of Plaintiff and the Class)

179. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

180. Plaintiff and Class members disclosed their highly sensitive PII/PHI to Defendant in confidence—with the implicit and explicit understanding that Defendant would collect, store, and protect their PII/PHI (and *not* allow the disclosure of their PII/PHI to unauthorized third parties).

181. As such, by obtaining (and continuing to maintain) Plaintiff's and Class members' PII/PHI, Defendant assumed an obligation to maintain the confidentiality of that PII/PHI.

182. At all times during the relationship between Defendant and Plaintiff and Class members, Defendant was fully aware of the highly confidential nature of Plaintiff's and Class members' PII/PHI.

183. Thus, Defendant intentionally, knowingly, and/or negligently committed the tort of breach of confidence by, *inter alia*:

a. failing to sufficiently encrypt or otherwise protect Plaintiff's and Class members' PII/PHI;

b. failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period;

c. and via the numerous instances of misconduct detailed *supra*.

184. As a direct and proximate result of Defendant's breach of confidence, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

WHEREFORE, Plaintiff and Class members respectfully request judgment against Defendant and that the Court enter an order:

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

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

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

D. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

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

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 other relief that this Court finds appropriate.

PRAYER FOR RELIEF

Plaintiff and Class members respectfully request judgment against Defendant and that the Court enter an order:

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

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

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

M. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

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

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

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

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

R. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Dated: February 28, 2024

Respectfully submitted,

SALTZ MONGELUZZI & BENDESKY, P.C.

By: */s/ Patrick Howard*
Patrick Howard, Esq. (PA ID #88572)
1650 Market Street, 52nd Floor
Philadelphia, PA 19103
Telephone: (215) 496-8282
phoward@smbb.com

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

**to be admitted pro hac vice*

Attorneys for Plaintiff and Proposed Class