UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

PETER LAZAR, on behalf of himself and all others similarly situated, Plaintiff, v. **INTERNATIONAL SHOPPES, LLC** and **DIPLOMATIC DUTY FREE SHOPS OF NEW YORK, INC**., Defendants.	No. 24-4170 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Peter Lazar ("Plaintiff"), through his attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendants International Shoppes, LLC and Diplomatic Duty Free Shops of New York, Inc. (together "Defendants"), and their 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 Defendants' failure to protect highly sensitive data.

2. Defendants are a "duty free and specialty retail operator in US based airports."[1]

3. As such, Defendants store a litany of highly sensitive personal identifiable information ("PII") and protected health information ("PHI")—together "PII/PHI"—about their

[1] *About Us*, INTERNATIONAL SHOPPES, https://ishoppes.com/pages/about-us (last visited May 12, 2024).

current and former employees, vendors, visitors, diplomatic customers, and foreign military customers.

4. But Defendants lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the "Data Breach").

5. It is unknown for precisely how long the cybercriminals had access to Defendants' network before the breach was discovered. In other words, Defendants had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to the PII/PHI of its current and former employees, vendors, visitors, diplomatic customers, and foreign military customers.

6. On information and belief, cybercriminals were able to breach Defendants' systems because Defendants 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, Defendants' failures placed the Class's PII/PHI in a vulnerable position—rendering them easy targets for cybercriminals.

7. Plaintiff is a Data Breach victim, having confirmed with Defendants that he was exposed. He brings this class action on behalf of himself, and all others harmed by Defendants' misconduct.

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

PARTIES

9. Plaintiff, Peter Lazar, is a natural person and citizen of New York. He resides in Seaford, New York where he intends to remain.

10. Defendant, International Shoppes, LLC, is a Limited Liability Company formed under the laws of New York and with its principal place of business at 540 Rockaway Avenue, Valley Stream, New York 11581. Upon information and belief, the members of International Shoppes, LLC are Michael Halpern and Stephen Greenbaum (both of which reside, and intend to remain, in New York).

11. Defendant, Diplomatic Duty Free Shops of New York, Inc., is a Foreign Business Corporation incorporated in Delaware and with its principal place of business at 540 Rockaway Avenue, Valley Stream, New York 11581.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Members of the proposed Class are citizens of different states than Defendants. And there are over 100 putative Class members.

13. This Court has personal jurisdiction over Defendants because it is headquartered in New York, regularly conducts business in New York, and has sufficient minimum contacts in New York.

14. Venue is proper in this Court because Defendants' principal offices are in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

BACKGROUND

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

15. Defendants is a "duty free and specialty retail operator in US based airports."[2]

16. As part of its business, Defendants receives and maintains the PII/PHI of thousands of its current and former employees, vendors, visitors, diplomatic customers, and foreign military customers.

17. In collecting and maintaining the PII/PHI, Defendants 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.

18. Under state and federal law, businesses like Defendants have duties to protect the PII/PHI of its current and former employees, vendors, visitors, diplomatic customers, and foreign military customers. Likewise, Defendants have duties to notify such individuals about any breaches.

19. Defendants recognizes these duties, declaring in its "Privacy Policy" that:

a. "This privacy policy provides the basis on which any personal information we collect from you or that you provide us will be used."[3]

b. "International Shoppes will not sell or disclose your personal information outside our corporate affiliates, except in connection with a joint venture or the proposed or actual sale of the whole or part of the business."[4]

[2] *About Us*, INTERNATIONAL SHOPPES, https://ishoppes.com/pages/about-us (last visited May 12, 2024).
[3] *Privacy Policy*, INTERNATIONAL SHOPPES, https://ishoppes.com/pages/privacy-policy (last visited May 12, 2024).
[4] *Id*.

c. "International Shoppes implements strict security measures to protect the information you provide us from access by unauthorized persons and against unlawful processing, accidental loss, destruction and damage."[5]

d. "[W]e will do our best to protect your personal information[.]"[6]

e. "You . . . will not hold us responsible for any breach of security unless we have been negligent."[7]

Defendants' Data Breach

20. On November 16, 2023, Defendants were hacked in a "ransomware attack."[8]

21. Worryingly, Defendants already admitted that "[t]he attacker appears to have [] ***obtained access*** to our systems."[9]

22. Notably, the "ransomware attack was discovered by [defendant's] employees after these employees reported that they were unable to access certain databases."[10]

23. And "[a]s part of the attack, [defendant's] systems were temporarily ***encrypted***."[11]

24. Because of Defendants' Data Breach, a broad range of PII/PHI was compromised.

25. For its current and former employees, Defendants exposed their:

a. addresses;

b. Social Security numbers;

---

[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] *Notice of Data Security Breach*, DEPT JUSTICE MONTANA (Feb. 8, 2024) https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-1088.pdf.
[9] *Id.* (emphasis added).
[10] *Id.*
[11] *Id.*

c. employment information (including salary information and performance reviews);

d. financial account numbers;

e. U.S. Airport SIDA IDs;

f. driver's license information;

g. passports and other government identification;

h. account credentials; and

i. health information.[12]

26. For its vendors and visitors, Defendants exposed their:

a. U.S. Airport SIDA IDs;

b. driver's license information; and

c. passports and other government identification.[13]

27. For its diplomatic and foreign military customers, Defendants exposed their:

a. work addresses;

b. home addresses;

c. other contact information (including email addresses and phone numbers);

d. purchasing information (including customer numbers, OFM PIDs, and approved OFM clearance forms);

e. copies of checks;

[12] *Id.*
[13] *Id.*

f. foreign military, foreign diplomatic, and government and other identifiers (including resident card information and identifications issued by the Office of Foreign Missions (OFM)).[14]

28. Currently, the precise number of persons injured is unclear. But upon information and belief, the size of the putative class can be ascertained from information in Defendants' custody and control. And upon information and belief, the putative class is over one hundred members—as it includes Defendants' current and former employees, vendors, visitors, diplomatic customers, and foreign military customers.

29. Still, Defendants were unable to detect its Data Breach until December 1, 2023—a full ***fifteen days*** after the Data Breach began.[15]

30. To make matters worse, Defendants then waited over until February 8, 2024, before it began notifying the class—a full 69 days after the Data Breach was discovered.[16]

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

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

a. "remain[] vigilant and review[] account statements and monitor[] free credit reports from consumer reporting agencies;"

b. "place a security freeze on your credit report;" and

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

c. "Contact the Federal Trade Commission . . . by mail at 600 Pennsylvania Avenue, NW, Washington, DC 20580; by phone at 1-877-ID-THEFT (877-438-4338); or online at www.consumer.gov/idtheft."[17]

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

34. Since the breach, Defendants have purportedly:

a. "taken a number of steps to mitigate potential harm and remediate the incident;"

b. "disabled remote access VPN connection;"

c. "restricted our network's access to the internet;"

d. "placed additional restrictions on user access to our network (including implementing multi-factor authentication and changing passwords for

e. certain systems);" and

f. "enhanced our network monitoring capabilities."[18]

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

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

[17] *Id.*
[18] *Id.*

37. Defendants have done little to remedy its Data Breach. True, Defendants have offered some victims credit monitoring.[19] But upon information and belief, such services are wholly insufficient to compensate Plaintiff and Class members for the injuries that Defendants inflicted upon them.

38. Because of Defendants' 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.

39. Worryingly, the cybercriminals that obtained Plaintiff's and Class members' PII/PHI appear to be the notorious cybercriminal group "LockBit."[20]

40. Arising in Russia during early 2020, LockBit is now "the most deployed ransomware variant across the world and continues to be prolific in 2023."[21]

41. Thus, the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), the Multi-State Information Sharing and Analysis Center (MS-ISAC) have warned that:

a. "LockBit affiliates have employed double extortion by first encrypting victim data and then exfiltrating that data while threatening to post that stolen data on leak sites."[22]

---

[19] *Id.*
[20] *See e.g.*, *Hacks of Today*, HACKMANAC (May 7, 2024) https://hackmanac.com/news/hacks-of-today-07-05-2024; *LockBit3*, RANSOMLOOK, https://www.ransomlook.io/group/lockbit3 (last visited May 12, 2024).
[21] *Cybersecurity Advisory*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (June 14, 2023) https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a.
[22] *Id.*

b. "Up to the Q1 2023, a total of 1,653 alleged victims were observed [i.e., published] on LockBit leak sites."[23]

42. And Reuters reports that:

a. "On the dark web, Lockbit's blog displays an ever-growing gallery of victim organisations that is updated nearly daily."[24]

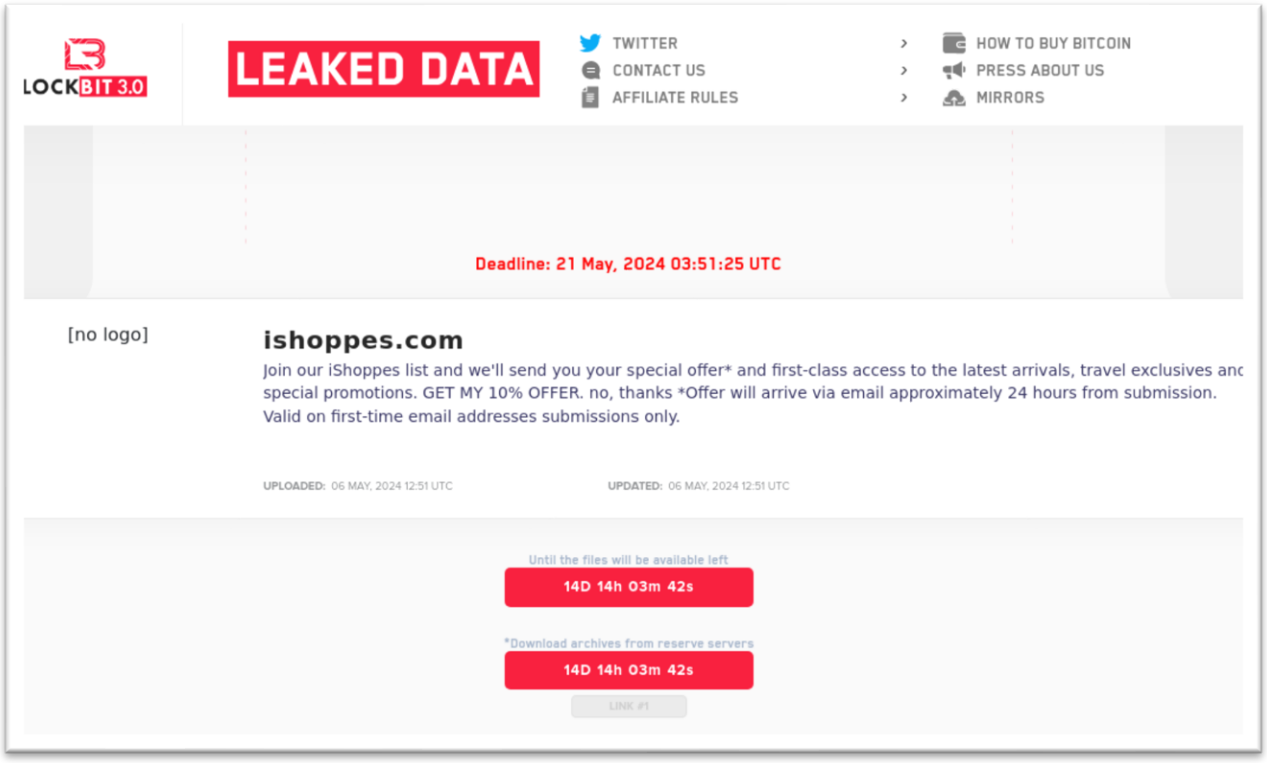
b. "Next to their names are digital clocks showing the number of days left to the deadline given to each organisation to provide ransom payment, failing which, the gang publishes the sensitive data it has collected."[25]

43. 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."[26]

44. Here, third-party reports have revealed that LockBit promised to ***publish*** the stolen PII/PHI by May 21, 2024—seemingly, unless the ransom is paid.[27] A screenshot of LockBit's Dark Web website is replicated below.[28]

---

[23] *Id*.
[24] Zeba Siddiqui & James Pearson, *Explainer: What is Lockbit? The digital extortion gang on a cybercrime spree*, REUTERS (Nov. 10, 2023) https://www.reuters.com/technology/cybersecurity/what-is-lockbit-digital-extortion-gang-cybercrime-spree-2023-11-10/.
[25] *Id*.
[26] 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.
[27] *See e.g.*, *Hacks of Today*, HACKMANAC (May 7, 2024) https://hackmanac.com/news/hacks-of-today-07-05-2024; *LockBit3*, RANSOMLOOK, https://www.ransomlook.io/group/lockbit3 (last visited May 12, 2024).
[28] *Id*. (providing screenshot of LockBit's Dark Web website).



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

Plaintiff's Experiences and Injuries

46. Plaintiff Peter Lazar is a former employee of Defendants—having worked for Defendants from approximately 2006 until 2014.

47. Thus, Defendants obtained and maintained Plaintiff's PII/PHI.

48. As a result, Plaintiff was injured by Defendants' Data Breach.

49. As a condition of his employment with Defendant, Plaintiff provided Defendants with his PII/PHI. Defendants 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.

50. Plaintiff provided his PII/PHI to Defendants and trusted the company would use reasonable measures to protect it according to Defendants' internal policies, as well as state and federal law. Defendants 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.

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

52. Defendants' council confirmed that Plaintiff's PII/PHI was exposed in the Data Breach.

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

54. Upon information and belief, through its Data Breach, Defendants compromised Plaintiff's:

a. addresses;

b. Social Security number;

c. employment information (including salary information and performance reviews);

d. financial account numbers;

e. U.S. Airport SIDA IDs;

f. driver's license information;

g. passports and other government identification;

h. account credentials; and

i. health information.

55. Notably, Plaintiff has ***already*** suffered from identity theft and fraud: two fraudulent charges on Plaintiff's Chase debit card (one for approximately $1,600.00 and the other for approximately $563.00) in or around April 2024; and

56. Regarding the fraudulent charges, Plaintiff spent a significant amount of time and effort communicating with Chase to get the fraudulent charges reimbursed.

57. Thereafter, Plaintiff was only reimbursed weeks after the fraudulent charges were placed. Thus, Plaintiff was unable to access those funds during the intervening time.

58. Additionally, because of fraudulent charges, Plaintiff was forced to close his Chase debit card—and thus was unable to readily access his account until he received a new debit card.

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

60. And in the aftermath of the Data Breach, Plaintiff has suffered from a spike in spam and scam text messages and phone calls (at least 1–2 per day).

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

62. Moreover, Plaintiff's credit score dropped by 34 points during November 2023 (the exact month of Defendants' Data Breach). Specifically, Plaintiff's credit score dropped by:

a. 25 points on November 4, 2023; and

b. 9 points on November 23, 2023.

63. These drops are fairly traceable to Defendants' Data Breach. After all, Defendants stated that "[t]he attacker ***appears*** to have first obtained access to our systems ***on or about*** November 16, 2023."[29]

64. Thus, the 9-point drop certainly occurred after the Data Breach began. And, upon information and belief, the 25-point drop also occurred after the Data Breach began (given that Defendants have not precisely determined when the Data Breach began).

65. Because of Defendants' 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.

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

67. 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 Defendants were required to adequately protect.

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

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

[29] *Notice of Data Security Breach*, DEPT JUSTICE MONTANA (Feb. 8, 2024) https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-1088.pdf (emphasis added).

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

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

71. Because of Defendants' 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 Defendants' possession—and is thus as risk for futures breaches so long as Defendants fails to take appropriate measures to protect the PII/PHI.

72. 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.

73. 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.

74. 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.

75. 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.).

76. 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.

77. 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.

78. Defendants disclosed the PII/PHI of Plaintiff and Class members for criminals to use in the conduct of criminal activity. Specifically, Defendants 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.

79. Defendants' 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.

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

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

81. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.[30]

82. 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."[31]

---

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

[31] 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.

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

Defendants Failed to Follow FTC Guidelines

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

85. 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.[32] 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.

86. 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.

87. 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;

[32] *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.

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.

88. 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 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.

89. In short, Defendants' failure to use reasonable and appropriate measures to protect against unauthorized access to the data—of its employees, vendors, visitors, and customers—constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendants Failed to Follow Industry Standards

90. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendants. 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.

91. 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.

92. Defendants 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.

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

Defendants Violated HIPAA

94. 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.[33]

95. 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.[34]

[33] 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.

[34] *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).

96. The Data Breach itself resulted from a combination of inadequacies showing Defendants failed to comply with safeguards mandated by HIPAA. Defendants' 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);

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 Defendants' 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).

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

CLASS ACTION ALLEGATIONS

98. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII/PHI was compromised in the Data Breach discovered by Defendants in December 2023, including all those individuals who received notice of the breach.

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

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

101. 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.

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

103. 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 100 members.

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

105. 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.

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

b. if Defendants 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 Defendants were negligent in maintaining, protecting, and securing PII/PHI;

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

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

f. if Defendants' 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.

107. 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 Defendants 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)

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

109. Plaintiff and the Class entrusted their PII/PHI to Defendants on the premise and with the understanding that Defendants would safeguard their PII/PHI, use their PII/PHI for business purposes only, and/or not disclose their PII/PHI to unauthorized third parties.

110. Defendants owed a duty of care to Plaintiff and Class members because it was foreseeable that Defendants' 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.

111. Defendants have 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.

112. Defendants owed these duties to Plaintiff and Class members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate security practices. After all, Defendants actively sought and obtained Plaintiff and Class members' PII/PHI.

113. Defendants 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.

114. Thus, Defendants 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.

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

116. Defendants 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.

117. Defendants' duty to use reasonable security measures arose because of the special relationship that existed between Defendants and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendants with their confidential PII/PHI, a necessary part of obtaining services from Defendants.

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

120. Defendants 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. Defendants' conduct was particularly unreasonable given the nature and amount of PII/PHI Defendants 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.

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

122. Defendants 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, Defendants' conduct was particularly unreasonable given the nature and amount of PHI that Defendants 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.

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

124. PII/PHI is highly valuable, and Defendants 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.

125. Defendants 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.

126. Defendants breached these duties as evidenced by the Data Breach.

127. Defendants 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.

128. Defendants 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.

129. Defendants 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.

130. Defendants have admitted that the PII/PHI of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

131. As a direct and traceable result of Defendants' 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.

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

133. Defendants' 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 Defendants' negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

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

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

135. Plaintiff and Class members were required to provide their PII/PHI to Defendants as a condition of receiving products, services, and/or employment provided by Defendants. Plaintiff and Class members provided their PII/PHI to Defendants or its third-party agents in exchange for Defendants' products, services, and/or employment.

136. Plaintiff and Class members reasonably understood that a portion of the funds they paid Defendants (or of the funds derived from their labor) would be used to pay for adequate cybersecurity measures.

137. Plaintiff and Class members reasonably understood that Defendants would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendants' duties under state and federal law and its internal policies.

138. Plaintiff and the Class members accepted Defendants' offers by disclosing their PII/PHI to Defendants or its third-party agents in exchange for products, services, and/or employment.

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

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

141. Implicit in the parties' agreement was that Defendants would provide Plaintiff and Class members with prompt and adequate notice of all unauthorized access and/or theft of their PII/PHI.

142. After all, Plaintiff and Class members would not have entrusted their PII/PHI to Defendants in the absence of such an agreement with Defendants.

143. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendants.

144. 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.

145. 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.

146. Defendants materially breached the contracts it entered with Plaintiff and Class members 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 Defendants created, received, maintained, and transmitted.

147. In these and other ways, Defendants violated its duty of good faith and fair dealing.

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

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

150. Plaintiff and Class members performed as required under the relevant agreements, or such performance was waived by Defendants' conduct.

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

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

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

153. Plaintiff and Class members conferred a benefit upon Defendants. After all, Defendants benefitted from:

a. using their PII/PHI to facilitate employment and/or the provision of goods and/or services; and/or

b. deriving profit from their payment for goods and/or services;

154. Defendants appreciated or had knowledge of the benefits it received from Plaintiff and Class members.

155. Plaintiff and Class members reasonably understood that Defendants would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendants' duties under state and federal law and its internal policies.

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

157. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendants 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 Defendants' failure to provide the requisite security.

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

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

160. Defendants 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.

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

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

162. Given the relationship between Defendants and Plaintiff and Class members, where Defendants became guardian of Plaintiff's and Class members' PII/PHI, Defendants 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) Defendants did and does store.

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

164. Because of the highly sensitive nature of the PII/PHI, Plaintiff and Class members would not have entrusted Defendants, or anyone in Defendants' position, to retain their PII/PHI had they known the reality of Defendants' inadequate data security practices.

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

166. Defendants 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.

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

FIFTH CAUSE OF ACTION
Violation of the New York Deceptive Trade Practices Act
New York Gen. Bus. Law § 349
(On Behalf of Plaintiff and the Class)

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

169. Section 349 of the New York Deceptive Trade Practices Act ("GBL") prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service[.]" N.Y. G.B.L. § 349(a).

170. Section 349 applies to Defendants because Defendants engage in "business, trade or commerce or in the furnishing of any service" within New York. *Id*.

171. Defendants violated § 349 by, *inter alia*:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' PII/PHI, which was a direct and proximate cause of the Data Breach;

b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. §

1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*., which was a direct and proximate cause of the Data Breach;

d. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII/PHI; and

e. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*.

172. Defendants' omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of their PII/PHI.

173. Defendants intended to mislead Plaintiff and Class members and induce them to rely on its omissions.

174. Had Defendants disclosed to Plaintiff and Class members that its data systems were not secure—and thus vulnerable to attack—Defendants would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendants accepted the PII/PHI that Plaintiff and Class members entrusted to it while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Class members acted reasonably in relying on Defendants' omissions, the truth of which they could not have discovered through reasonable investigation.

175. Defendants acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiff's and Class members' rights.

176. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiff and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII/PHI.

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

178. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law.

SIXTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

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

180. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

181. In the fallout of the Data Breach, an actual controversy has arisen about Defendants' various duties to use reasonable data security. On information and belief, Plaintiff alleges that Defendants' actions were—and *still* are—inadequate and unreasonable. And Plaintiff and Class members continue to suffer injury from the ongoing threat of fraud and identity theft.

182. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendants have a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendants breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendants breaches of its duties caused—and continues to cause—injuries to Plaintiff and Class members.

183. The Court should also issue corresponding injunctive relief requiring Defendants to use adequate security consistent with industry standards to protect the data entrusted to it.

184. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendants experiences a second data breach.

185. And if a second breach occurs, Plaintiff and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiff and Class members' injuries.

186. If an injunction is not issued, the resulting hardship to Plaintiff and Class members far exceeds the minimal hardship that Defendants could experience if an injunction is issued.

187. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class members, and the public at large.

PRAYER FOR RELIEF

Plaintiff and Class members respectfully request judgment against Defendants 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. Enjoining Defendants from further unfair and/or deceptive practices;

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

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

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

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

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

J. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Date: June 11, 2024

Respectfully submitted,

By: /s/ James J. Bilsborrow
James J. Bilsborrow
WEITZ & LUXENBERG, PC
700 Broadway
New York, NY 10003
T: (212) 558-5500
jbilsborrow@weitzlux.com

Samuel J. Strauss*
Raina C. Borrelli*
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
T: (872) 263-1100
F: (872) 263-1109
sam@straussborrelli.com
raina@straussborrelli.com

**Pro hac vice forthcoming*
Attorneys for Plaintiff and Proposed Class

JS 44 (Rev. 03/24)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

Peter Lazar

(b) County of Residence of First Listed Plaintiff Nassau
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

James J Bilsborrow, Weitz & Luxenberg, PC
700 Broadway, New York, NY 10003, 212-558-5500

DEFENDANTS

International Shoppes, LLC and Diplomatic Duty Free Shops of New York, Inc.

County of Residence of First Listed Defendant Nassau
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☒ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☒ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

INTELLECTUAL PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 USC 1332(d)

Brief description of cause:
Unlawful breach of personal identifying information

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
06/11/2024

SIGNATURE OF ATTORNEY OF RECORD
/s/ James J. Bilsborrow

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

CERTIFICATION OF ARBITRATION ELIGIBILITY

Local Arbitration Rule 83.7 provides that with certain exceptions, actions seeking money damages only in an amount not in excess of $150,000, exclusive of interest and costs, are eligible for compulsory arbitration. The amount of damages is presumed to be below the threshold amount unless a certification to the contrary is filed.

Case is Eligible for Arbitration ☐

I, _____, counsel for_____, do hereby certify that the above captioned civil action is ineligible for compulsory arbitration for the following reason(s):

☐ monetary damages sought are in excess of $150,000, exclusive of interest and costs,

☐ the complaint seeks injunctive relief,

☐ the matter is otherwise ineligible for the following reason

DISCLOSURE STATEMENT - FEDERAL RULES CIVIL PROCEDURE 7.1

Identify any parent corporation and any publicly held corporation that owns 10% or more or its stocks:

RELATED CASE STATEMENT (Section VIII on the Front of this Form)

Please list all cases that are arguably related pursuant to Division of Business Rule 3 in Section VIII on the front of this form. Rule 3(a) provides that "A civil case is "related" to another civil case for purposes of this guideline when, because of the similarity of facts and legal issues or because the cases arise from the same transactions or events, a substantial saving of judicial resources is likely to result from assigning both cases to the same judge and magistrate judge." Rule 3(a) provides that " A civil case shall not be deemed "related" to another civil case merely because the civil case involves identical legal issues, or the same parties." Rule 3 further provides that
"Presumptively, and subject to the power of a judge to determine otherwise pursuant to paragraph (b), civil cases shall not be deemed to be "related" unless both cases are still pending before the court."

NY-E DIVISION OF BUSINESS RULE 1(d)

1.) Is the civil action being filed in the Eastern District removed from a New York State Court located in Nassau or Suffolk County? ☐ Yes ☑ No

2.) If you answered "no" above:
a) Did the events or omissions giving rise to the claim or claims, or a substantial part thereof, occur in Nassau or Suffolk County? ☑ Yes ☐ No

b) Did the events or omissions giving rise to the claim or claims, or a substantial part thereof, occur in the Eastern District? ☑ Yes ☐ No

c) If this is a Fair Debt Collection Practice Act case, specify the County in which the offending communication was received: .

If your answer to question 2 (b) is "No," does the defendant (or a majority of the defendants, if there is more than one) reside in Nassau or Suffolk County, or, in an interpleader action, does the claimant (or a majority of the claimants, if there is more than one) reside in Nassau or Suffolk County? ☐ Yes ☐ No

(Note: A corporation shall be considered a resident of the County in which it has the most significant contacts).

BAR ADMISSION

I am currently admitted in the Eastern District of New York and currently a member in good standing of the bar of this court.

☑ Yes ☐ No

Are you currently the subject of any disciplinary action (s) in this or any other state or federal court?

☐ Yes (If yes, please explain ☑ No

I certify the accuracy of all information provided above.

Signature: James Bilsborrow

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Eastern District of New York

Peter Lazar, on behalf of himself and all others similarly situated,

Plaintiff(s)

v.

International Shoppes, LLC and Diplomatic Duty Free Shops of New York, Inc.

Defendant(s)

Civil Action No. 24-4170

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* International Shoppes, LLC
540 Rockaway Avenue
Valley Stream, NY 11581

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: James J Bilsborrow
Weitz & Luxenberg PC
700 Broadway
New York, NY 10003

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

BRENNA B. MAHONEY
CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No. 24-4170

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

Print Save As... Reset

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Eastern District of New York

Peter Lazar, on behalf of himself and all others similarly situated

Plaintiff(s)

v.

International Shoppes, LLC and Diplomatic Duty Free Shops of New York, Inc.

Defendant(s)

Civil Action No. 24-4170

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* Diplomatic Duty Free Shops of New York, Inc.
540 Rockaway Avenue
Valley Stream, NY 11581

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: James J. Bilsborrow
Weitz & Luxenberg, PC
700 Broadway
New York, NY 10003

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

BRENNA B. MAHONEY
CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No. 24-4170

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____

was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____

_____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____

_____ , a person of suitable age and discretion who resides there,

on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is

designated by law to accept service of process on behalf of *(name of organization)* _____

_____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____

Server's signature

_____

Printed name and title

_____

Server's address

Additional information regarding attempted service, etc:

Print Save As... Reset