UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SAMANTHA WILLIAMS, on behalf of herself and all others similarly situated, Plaintiff, v. **WATERGATE HOTEL, LLC and EURO CAPITAL PROPERTIES, LLC**, Defendants.	No. 1:26-cv-1399 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Samantha Williams ("Plaintiff"), through her attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendants Watergate Hotel, LLC ("Watergate") and Euro Capital Properties, LLC ("Euro Capital") (collectively "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 her 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. Defendant Watergate is a luxury hotel located in Washington D.C.[1]

[1] *About the Watergate*, THE WATERGATE HOTEL, https://www.thewatergatehotel.com/about (last visited Feb. 6, 2026).

3. Defendant Euro Capital is an international hotel real estate development and management company.[2]

4. As such, Defendants store a litany of highly sensitive personal identifiable information ("PII") about their current and former employees and consumers. But Defendants lost control over that data when cybercriminals infiltrated their 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 their systems—thereby allowing cybercriminals unrestricted access to their current and former employees' and consumers' PII.

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

7. Plaintiff is a Data Breach victim, having received a breach notice. A sample of the breach notice sent by Defendants is attached as Exhibit A. She brings this class action on behalf of herself, and all others harmed by Defendants' misconduct.

8. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before this data breach, their current and former employees and consumers' private information was

[2] *About Us*, EURO CAPITAL PROPERTIES, https://eurocapprop.com/about-us/ (last visited Feb. 18, 2026).

exactly that—private. Not anymore. Now, their private information is forever exposed and unsecure.

PARTIES

9. Plaintiff, Samantha Williams, is a natural person and a citizen of Washington, D.C., where she intends to remain.

10. Defendant, Watergate Hotel, LLC, is a limited liability company organized in Delaware and with its principal place of business at 152 West 57th Street New York, New York 10019.

11. Defendant, Euro Capital Properties, LLC, is a limited liability company organized in Delaware and with its principal place of business at 152 West 57th Street New York, New York 10019.

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. Plaintiff and Defendants are citizens of different states. [3] And there are over 100 putative Class Members.

13. This Court has personal jurisdiction over Defendants because they are headquartered in New York, regularly conduct business and have sufficient minimum contacts in New York.

[3] Under the Class Action Fairness Act, "an unincorporated association shall be deemed to be a citizen of the State where it has its principal place of business and the State under whose laws it is organized." 28 U.S.C. § 1332(d)(10);

14. Venue is proper in this Court because Defendants' principal office is 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 of Plaintiff and the Class

Watergate

15. Defendant Watergate is "an iconic landmark" and luxury hotel located in Washington D.C.[4]

16. As part of its business, Watergate receives and maintains the PII of thousands of its current and former employees and consumers.

17. In collecting and maintaining the PII, Watergate 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.

18. Under state and federal law, businesses like Watergate have duties to protect its current and former employees and consumers' PII and to notify them about breaches.

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

a. "We recognize that privacy is important to our guests, and hence it is important to us."[5]

---

[4] *About the Watergate*, THE WATERGATE HOTEL, https://www.thewatergatehotel.com/about (last visited Feb. 6, 2026).
[5] *Privacy Policy & Security*, THE WATERGATE HOTEL, https://www.thewatergatehotel.com/privacy-policy-security (last visited Feb. 6, 2026).

b. "We have implemented a security program which is designed to keep information that is stored in our systems protected from unauthorized access or use."[6]

c. "We use reasonable technological, physical and other security measures to protect your personal information from unauthorized access."[7]

d. "For example, the website servers and systems are configured with data encryption or scrambling technologies and industry standard firewalls, and when you enter personal information during the reservation process, your data is protected by Secure Socket Layer (SSL)."[8]

Euro Capital

20. Defendant Euro Capital is an international hotel real estate development and management company.[9]

21. Euro Capital claims to be "committed to growing our reputation as one of distinguished, secure and innovative."[10]

22. The Watergate Hotel is one of Euro Capital's hotel management projects.[11]

23. As part of its business, Euro Capital receives and maintains the PII of thousands of Watergate's current and former employees and consumers.

---

[6] *Id*.
[7] *Id*.
[8] *Id*.
[9] *About Us*, EURO CAPITAL PROPERTIES, https://eurocapprop.com/about-us/ (last visited Feb. 18, 2026).
[10] *Id*.
[11] *Development*, EURO CAPITAL PROPERTIES, https://eurocapprop.com/development/ (last visited Feb. 18, 2026).

24. In collecting and maintaining the PII, Euro Capital 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.

25. Under state and federal law, businesses like Euro Capital have duties to protect its current and former employees and consumers' PII and to notify them about breaches.

Defendants' Data Breach

26. On or around April 6, 2024, Watergate was hacked in the Data Breach.[12]

27. Worryingly, Watergate already admitted that "through [Watergate's] investigation, we determined that an unknown actor gained access to computer systems on our network and was able to view or download certain files."[13]

28. Because of Defendants' Data Breach, at least the following types of PII were compromised:

a. Name;

b. Social Security number;

c. Driver's license and/or other government issued identification number;

d. Financial account information; and

e. Payment card information

29. In total, Defendants injured at least 2,200 persons—via the exposure of their PII—in the Data Breach.[14] Upon information and belief, these 2,200 persons include their current and former employees and consumers.

---

[12] *See* Exhibit A.
[13] *Id.*
[14] *Data Breach Notifications*, OFFICE OF THE MAINE ATTORNEY GENERAL, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/d97e9375-1220-433b-a9f5-0c699a7f0d62.html (last visited Feb. 6, 2026).

30. And yet, Defendants waited until February 7, 2025, before they began notifying the class—a full 307 days after the Data Breach began.[15]

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. "We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and free credit reports for suspicious activity and to detect errors."[16]

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

34. Since the breach, Defendants claim that "[u]pon becoming aware of the activity, we immediately took steps to secure our systems and initiated a comprehensive response."[17]

35. But such simple declarations are insufficient to ensure that Plaintiff's and Class Members' PII will be protected from additional exposure in a subsequent data breach.

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

---

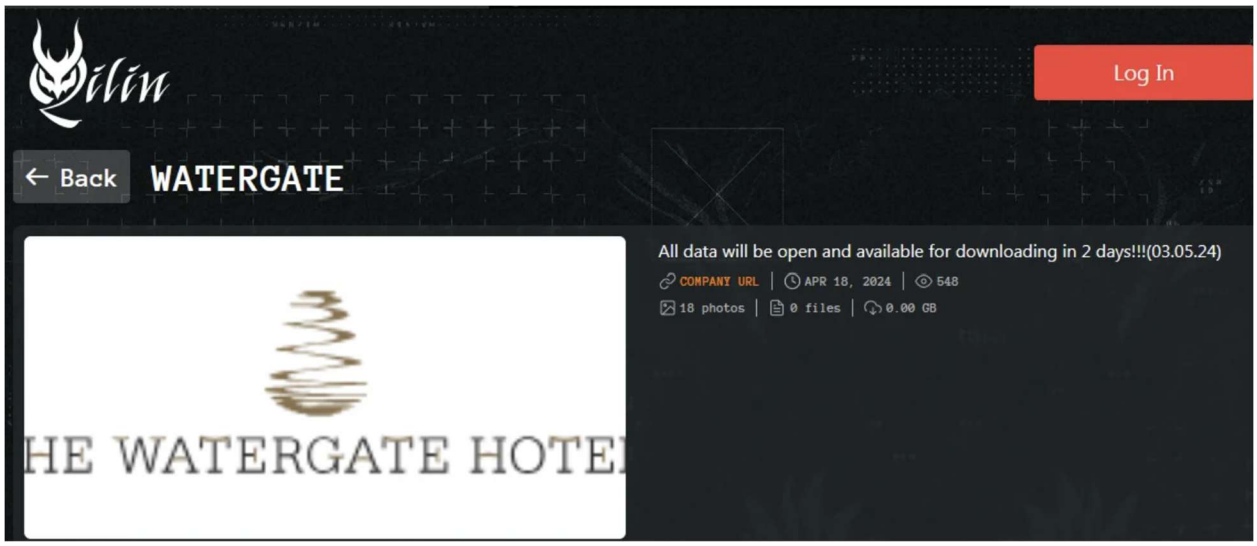
[15] *See* Exhibit A.
[16] *Id.*
[17] *Id.*

37. Defendants have done little to remedy the Data Breach. True, Defendants have 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 Defendants inflicted upon them.

38. Because of Defendants' Data Breach, the sensitive PII of Plaintiff and Class Members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class Members.

Qilin & the Dark Web

39. Worryingly, the cybercriminals that obtained Plaintiff's and Class Members' PII appear to be the notorious cybercriminal group "Qilin."[18]



[18] *The Watergate Hotel Data Breach*, BREACH SENSE, https://www.breachsense.com/breaches/the-watergate-hotel-data-breach/ (last visited Feb. 6, 2026).

40. Qilin is an especially notorious cybercriminal group. In fact, Qilin is "a serious threat to businesses and critical infrastructure worldwide" that incorporates "advanced techniques in malware construction and evasion."[19]

41. Upon information and belief, the cybercriminals in question are particularly sophisticated. After all, the cybercriminals: (1) defeated the relevant data security systems, (2) gained actual access to sensitive data, and (3) successfully accessed and acquired data.

42. 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."[20]

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

Plaintiff's Experiences and Injuries

44. Plaintiff Samantha Williams is a former employee of Watergate.

45. Thus, Defendants obtained and maintained Plaintiff's PII.

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

47. Plaintiff is very careful about the privacy and security of her PII. She does not knowingly transmit her PII over the internet in an unsafe manner. She is careful to store any documents containing her PII in a secure location.

---

[19] Andrew Doyle, *Qilin Ransomware: Tactics, Techniques, Procedures and Mitigation*, SECURITY DAILY REVIEW (Apr. 23, 2025), https://dailysecurityreview.com/resources/qilin-ransomware-tactics-techniques-procedures-and-mitigation/

[20] 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.

48. As a condition of her employment with Watergate, Plaintiff provided Defendants with her PII. Defendants used that PII to facilitate their employment of Plaintiff, including payroll, and required Plaintiff to provide that PII in order to obtain employment and payment for that employment.

49. Plaintiff provided her PII 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 continue to maintain Plaintiff's PII and have a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

50. Plaintiff reasonably understood that a portion of the funds derived from her employment with Defendants would be used to pay for adequate cybersecurity and protection of PII.

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

52. Plaintiff received a Notice of Data Breach dated February 7, 2025.

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

54. Through their Data Breach, Defendants compromised Plaintiff's PII.

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

56. And in the aftermath of the Data Breach, Plaintiff suffered from a spike in spam and scam emails, text messages and phone calls.

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

58. 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.

59. Plaintiff suffered actual injury from the exposure and theft of her PII—which violates her rights to privacy.

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

61. 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 right in the hands of criminals.

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

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

Consumers Prioritize Data Security

64. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."[21] Therein, Cisco reported the following:

a. "For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't trust with their data."[22]

b. "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly."[23]

c. 89% of consumers stated that "I care about data privacy."[24]

d. 83% of consumers declared that "I am willing to spend time and money to protect data" and that "I expect to pay more" for privacy.[25]

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[26]

f. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."[27]

Plaintiff and the Proposed Class Suffered Common Injuries and Damages

---

[21] *Privacy Awareness: Consumers Taking Charge to Protect Personal*, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited March 19, 2025).
[22] *Id*. at 3.
[23] *Id*.
[24] *Id*. at 9.
[25] *Id*.
[26] *Id*.
[27] *Id*. at 11.

65. 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 is used;

b. diminution in value of their PII;

c. compromise and continuing publication of their PII;

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; and

h. continued risk to their PII—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.

Substantially Increased Risk of Identity Theft and Fraud

66. Plaintiff and Class Members are at a heightened risk of identity theft for years to come because of the Data Breach.

67. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201 (2013).

68. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

69. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal individuals' personal data to monetize the information. Criminals monetize the data by selling the stolen information on the internet black market (aka the Dark Web) to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

70. The "Dark Web" is an unindexed layer of the internet that requires special software or authentication to access.[28] Criminals in particular favor the Dark Web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, Dark Web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the Dark Web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[29] This prevents Dark Web marketplaces from being easily monitored by authorities or accessed by those not in the know.

71. The unencrypted PII of Plaintiff and Class Members has or will end up for sale on the Dark Web because that is the modus operandi of hackers. In addition, unencrypted and detailed PII may fall into the hands of companies that will use it for targeted marketing without the approval

---

[28] *What Is the Dark Web?*, EXPERIAN, https://www.experian.com/blogs/ask-experian/what-isthe-dark-web/ (last visited July 9, 2025).
[29] *Id*.

of Plaintiff and Class Members. Unauthorized individuals can easily access the Plaintiff's and Class Members' PII.

72. Theft of Social Security numbers also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of their SSN, and a new SSN will not be provided until after the victim has suffered the harm.

73. In particular, the theft of Social Security numbers—in combination with other PII (e.g., name, address, date of birth)—provides cybercriminals with a "skeleton key" to commit rampant fraud and identity theft.

74. For example, cybersecurity expert Jim Stickley explained to Time Magazine that "[i]f I have your name and your Social Security number, and you haven't gotten a credit freeze yet, you're easy pickings . . . With that, you can do whatever you want . . . You can become that person."[30] For context, Jim Stickley is a "penetration tester" who is employed by businesses "to infiltrate their systems in order to find flaws they can fix before the bad guys exploit them."[31]

75. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years later. An individual may not know that their Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected

---

[30] Patrick L. Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME MAGAZINE (Aug. 5, 2019) https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[31] *Id.*

fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

76. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[32]

77. It is within this context that Plaintiff and all other Class Members must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

78. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or to track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

79. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

---

[32] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. SYSTEMICS, CYBERNETICS & INFORMATICS 9 (2019) http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

80. Identity thieves can also use an individual's personal data and PII to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's information, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant issued in the victim's name.[33]

81. One example of criminals piecing together bits and pieces of compromised PII to create comprehensive dossiers on individuals is called "Fullz" packages.[34] These dossiers are both shockingly accurate and comprehensive. With "Fullz" packages, cybercriminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals. For example, they can combine the stolen PII, and with unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

---

[33] *Identity Theft and Your Social Security Number,* SOCIAL SECURITY ADMINISTRATION, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf. (last visited July 9, 2025).

[34] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm,* KREBS ON SECURITY (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/ medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm.

82. The development of "Fullz" packages means that the PII exposed in the Data Breach can easily be linked to data of Plaintiff and the Class that is available on the internet. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII 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 is being misused, and that such misuse is fairly traceable to the Data Breach.

83. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[35]

84. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Yet Defendants failed to rapidly report to Plaintiff and the Class that their PII was stolen. Defendants' failure to promptly and properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff's and Class Members' injuries by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

85. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

---

[35] *2019 Internet Crime Report* (Feb. 11, 2020) FED. BUREAU INTELLIGENCE, https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last visited July 9, 2025).

86. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

87. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and Class Members will need to remain vigilant for years or even decades to come.

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

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

89. In 2024, a record 3,158 data breaches occurred—exposing approximately 1,350,835,988 sensitive records (i.e., 211% increase year over year).[36]

90. 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."[37]

91. Therefore, the increase in such attacks, and attendant risk of future attacks, was

---

[36] *2024 Data Breach Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2025), https://www.idtheftcenter.org/wp-content/uploads/2025/02/ITRC_2024DataBreachReport.pdf.
[37] 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.

widely known to the public and to anyone in Defendants' industry, including Defendants.

Defendants Could Have Prevented the Data Breach

92. Data breaches are preventable.[38] Indeed, the American Bar Association published a treatise titled the *Data Breach and Encryption Handbook* wherein the author explained that:

a. "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[39]

b. "Organizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised[.]"[40]

c. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures . . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs." [41]

Defendants Failed to Follow FTC Guidelines

93. 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 Defendants—should use to protect against unlawful data exposure.

---

[38] Lucy L. Thomson, *Despite the Alarming Trends, Data Breaches Are Preventable*, DATA BREACH AND ENCRYPTION HANDBOOK (2012).
[39] *Id.* at 17.
[40] *Id.* at 28.
[41] *Id.*

94. 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.[42] 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.

95. 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.

96. 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.

97. 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

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

U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

98. In short, Defendants' failure to use reasonable and appropriate measures to protect against unauthorized access to their current and former employees and consumers' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendants Failed to Follow Industry Standards

99. 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.

100. 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.

101. Upon information and belief, Defendants failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

102. 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.

CLASS ACTION ALLEGATIONS

103. 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 was compromised in the Data Breach discovered by Defendants in April 2024, including all those individuals who received notice of the breach.

104. Excluded from the Class are Defendants, their agents, affiliates, parents, subsidiaries, any entity in which Defendants has 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.

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

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

107. 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.

108. 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 2,200 members.

109. 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.

110. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's common interests. Her 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.

111. 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;

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;

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

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.

112. 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)

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

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

115. 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 in a data breach. And here, that foreseeable danger came to pass.

116. Defendants have full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if their PII was wrongfully disclosed.

117. 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.

118. Defendants owed—to Plaintiff and Class Members—at least the following duties to:

a. exercise reasonable care in handling and using the PII in their 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.

119. 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, 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.

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

121. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII 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.

122. 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, a necessary part of obtaining services from Defendants.

123. 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.

124. 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 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.

125. Defendants violated their duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII 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.

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

127. PII is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and Class Members' and the importance of exercising reasonable care in handling it.

128. Defendants improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

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

130. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members' PII by:

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

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

131. Defendants breached their duties by failing to exercise reasonable care in supervising their agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff and Class Members' injury.

132. Defendants further breached their 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.

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

134. 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.

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

136. Defendants' breach of their common-law duties to exercise reasonable care and their 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 by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, 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)

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

138. Plaintiff and Class Members were required to provide their PII to Defendants as a condition of receiving services and employment provided by Defendants. Plaintiff and Class

Members provided their PII to Defendants or their third-party agents in exchange for Defendants' services and employment.

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

140. Plaintiff and Class Members reasonably understood that Defendants would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendants' duties under state and federal law and their internal policies.

141. Plaintiff and the Class Members accepted Defendants' offers by disclosing their PII to Defendants or their third-party agents in exchange for services and employment.

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

143. 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.

144. After all, Plaintiff and Class Members would not have entrusted their PII to Defendants in the absence of such an agreement with Defendants.

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

146. 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.

147. 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.

148. 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 their 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 that Defendants created, received, maintained, and transmitted.

149. In these and other ways, Defendants violated their duty of good faith and fair dealing.

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

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

152. 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)

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

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

155. Plaintiff and Class Members conferred a benefit upon Defendants. After all, Defendants benefitted from (1) using their PII to provide services or facilitate employment, and (2) accepting payment or using their labor to derive profit.

156. Defendants appreciated or had knowledge of the benefits they received from Plaintiff and Class Members.

157. Plaintiff and Class Members reasonably understood that Defendants would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendants' duties under state and federal law and their internal policies.

158. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

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

160. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiff's and Class Members' (1) PII and (2) employment or payment because Defendants failed to adequately protect their PII.

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

162. 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 their misconduct.

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

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

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

165. As such, by obtaining (and continuing to maintain) Plaintiff's and Class Members' PII, Defendants assumed an obligation to maintain the confidentiality of that PII.

166. At all times during the relationship between Defendants and Plaintiff and Class Members, Defendants were fully aware of the highly confidential nature of Plaintiff's and Class Members' PII.

167. Thus, Defendants 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;

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*.

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

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

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

170. Under the New York Gen. Bus. Law § 349, "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful."

171. Section § 349 applies to Defendants because there is a sufficient nexus between Defendants' conduct and New York. After all, Defendants' headquarters is in New York. And upon information and belief, the deceptive acts or practices discussed herein occurred and/or were authorized in New York.

172. Defendants' deceptive acts and/or practices were directed at consumers because Defendants' privacy policy represented to consumers that it would use reasonable data security.

173. Such representations were deceptive because they induced consumers to disclose their PII.

174. Additionally, Defendants' deceptive acts and/or practices were directed at consumers because Defendants failed to notify consumers about their Data Breach in a reasonable and timely manner.

175. Furthermore, Defendant violated § 349 by, inter alia:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' PII, 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, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the FCRA, 15 U.S.C. § 1681e, 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; 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, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the FCRA, 15 U.S.C. § 1681e.

176. 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.

177. Defendants intended to mislead Plaintiff and Class Members and induce them to rely on their omissions.

178. Had Defendants disclosed to Plaintiff and Class Members that their 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 that Plaintiff and Class Members entrusted to them while keeping the inadequate state of their 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.

179. Defendants acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiff's and Class Members' rights. 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.

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

181. 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)

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

183. 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.

184. 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.

185. 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 them;

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 continue to breach, their duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendants' breaches of their duties caused—and continue to cause—injuries to Plaintiff and Class Members.

186. 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.

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

188. 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.

189. 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.

190. 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 her 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.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Date: February 18, 2026

Respectfully submitted,

/s/__Linda H. Joseph_____

Linda H. Joseph, Esq.
SCHRÖDER, JOSEPH & ASSOCS. LLP
394 Franklin Street, Second Floor
Buffalo, New York 14202
(716) 881-4900
(716) 881-4909 (facsimile)
(716) 861-1398 (cell)
ljoseph@sjalegal.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

Exhibit A

THE WATERGATE HOTEL
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

February 7, 2025

M7856-L01-0000001 P001 T00001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 INDIVIDUAL
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

Notice of Data [Incident/Breach]

Dear Sample A. Sample:

The Watergate Hotel ("Watergate") is writing to inform you of an event that may have affected the security of certain information related to you. This notice provides information about the event, our response, and resources available to you to help protect your information should you feel it appropriate to do so.

What Happened? On April 6, 2024, Watergate identified suspicious activity on our network. We immediately took steps to secure our environment and launched an investigation into the nature and scope of the activity. Through our investigation, we determined that an unknown actor gained access to computer systems on our network and was able to view or download certain files. Following this determination, we undertook a comprehensive review of the files determined to be at risk to assess the information contained therein and to whom it relates. On December 9, 2024, we completed this review and determined that the impacted dataset contained information related to you.

What Information Was Involved? The information potentially impacted includes your: [data elements].

What We Are Doing. The confidentiality, privacy, and security of information in our care are among our highest priorities. Upon becoming aware of the activity, we immediately took steps to secure our systems and initiated a comprehensive response. We also promptly notified federal law enforcement, and reviewed our security policies and procedures to reduce the risk of similar future events.

As an added precaution, we are offering you access to complimentary credit monitoring and identity restoration services for ## months through Experian. Enrollment instructions are enclosed with this letter.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and free credit reports for suspicious activity and to detect errors. Additional information and resources are included in the enclosed *Steps You Can Take to Help Protect Personal Information*. You may also enroll in the complementary credit monitoring services we have made available to you.

For More Information. If you have questions, please call our toll-free assistance line at 833-918-7947, Monday through Friday from 9 am – 9 pm Eastern (excluding U.S. holidays). You may also write to Watergate at 2650 Virginia Avenue NW, Washington, DC 20037.

Sincerely,

Abe Liao
Managing Director
The Watergate Hotel

0000001

ENGAGE#

M7856-L01

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for ## months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for ## months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary ##-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** April 30, 2025 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/credit
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-918-7947 by April 30, 2025. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR ##-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/get-credit-report https://www.transunion.com/credit-freeze https://www.transunion.com/fraud-alerts
888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, PO Box 2000 Chester, PA 19016

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania

Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. To file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.