UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

BEVERLY ANDERSON on behalf of herself and all others similarly situated, Plaintiff, v. RENEWAL BY ANDERSEN LLC, RENEWAL BY ANDERSEN OF THE GREATER TWIN CITIES, RENEWAL BY ANDERSEN OF THE TWIN CITIES, Defendants.	Case No. 0:23-cv-1886 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff, Beverly Anderson, through her attorneys, brings this Class Action Complaint against the Defendant, Renewal By Andersen LLC, Renewal By Andersen of the Greater Twin Cities, Renewal By Andersen of the Twin Cities ("Renewal" or "Defendant"), alleging as follows:

INTRODUCTION

1. In 2023, Renewal, a company specializing in window and door replacement, discovered it had lost control over its computer network and the highly sensitive private information stored on the computer network in a data breach perpetuated by cybercriminals ("Data Breach"). The number of total breach victims is unknown, but on information and belief, the Data Breach has impacted at least thousands of former and current customers.

2. On information and belief, Defendant was discovered the Data Breach in January 2023, when an unauthorized party gained access to Defendant's network. Following an internal investigation, Defendant learned that its systems had been unsecured between January 2018, and

January 19, 2023, allowing cybercriminals unfettered access to former and current customers' personally identifiable information ("PII"), including but not limited to their names, Social security number, driver's license number, address, banking account number, routing number, and credit card number, for an appalling *five years*.

3. On or around May 12, 2023– four months after Defendant first became aware of the Data Breach and a shocking five and a half years after cybercriminals first gained unauthorized access to Defendant's system – Defendant finally began notifying victims about the breach (the "Breach Notice") an example which is attached as **Exhibit A**. However, Renewal has not yet completed notice and continues to notify breach victims.

4. Plaintiff did not receive a Notice Letter from Renewal but had to instead be notified through Intuit that her PII was exposed due to the Data Breach. During this time, Plaintiff and Class Members were unaware that their PII had been compromised and published online, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

5. Renewal failed to reasonably secure, monitor, and maintain the PII provided to it by its former and current customers. Upon information and belief, the Data Breach resulted in the likely unauthorized access, download, exfiltration, and misuse of the PII by the cyber criminals who targeted that information through their wrongdoing.

6. Defendant's Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell its victims how many people were impacted, how the breach happened, or why it took the Defendant five and a half years to discover the breach and four months to begin notifying some of its victims that hackers had gained access to highly sensitive PII.

7. Defendant's failure to timely detect and report the Data Breach made its customers

vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

8. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

9. In failing to adequately protect customers' information, adequately notify them about the breach, and obfuscating the nature of the breach, Defendant violated state law and harmed an unknown number of its former and current customers.

10. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and the Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

11. Plaintiff is a former Renewal customer and a Data Breach victim.

12. Accordingly, Plaintiff, on behalf of herself and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

PARTIES

13. Plaintiff, Beverly Anderson, is a natural person and citizen of Michigan, residing in Grand Haven, Michigan, where she intends to remain. Ms. Anderson is a Data Breach victim.

14. Defendant, Renewal By Andersen LLC, is a corporation with its principal place of business at 551 North Maine Street Bayport, MN 55003.

15. Defendant, Renewal By Andersen of the Greater Twin Cities, is a corporation with its principal place of business at 551 North Maine Street Bayport, MN 55003.

16. Defendant, Renewal By Andersen of the Twin Cities, is a corporation with its principal place of business at 551 North Maine Street Bayport, MN 55003.

JURISDICTION & VENUE

17. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class; Plaintiff and Defendant are citizens of different states.

18. Renewal is incorporated in and maintains its principal place of business in Minnesota at 551 North Maine Street Bayport, MN 55003. Renewal is thus a Minnesota citizen.

19. This Court has personal jurisdiction over Renewal because it is a citizen in this District and maintains its headquarters and principal place of business in this District.

20. Venue is proper because Renewal maintains its headquarters and principal place of business in this District.

BACKGROUND FACTS

Renewal

21. Renewal is a construction and manufacturing company specializing in window and door replacement with 7 company owned locations and over 100 affiliates across the United States. Renewal touts that it "is committed to giving you the best customer experience possible, through the perfect combination of thebest [*sic*] people in the industry, a superior process, and an exclusive product."[1]

22. On information and belief, Renewal accumulates highly sensitive PII Information of its customers.

[1] Why Renewal, Renewal by Andersen, https://www.renewalbyandersen.com/signature-service (last visited June 20, 2023).

23. On information and belief, Renewal maintains former and current customers' PII for years after the customer's relationship with Defendant is terminated.

24. According to its website, Renewal promises that it "takes reasonable and appropriate steps to protect your Personal Information from unauthorized access, use, or disclosure", stating that "access to and use of secure areas of our sites is restricted to authorized users only with a business need to know the Personal Information accessible there.[2]

25. Renewal understood the need to protect its customers' data and prioritize its data security. However, despite recognizing its duty to do so, on information and belief, Renewal has not in fact implemented reasonably cybersecurity safeguards or policies to protect its customers' PII or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Renewal leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to former and current customers' PII.

Renewal Fails to Safeguard Customer PII

26. Plaintiff is a former customer of Renewal.

27. As a condition of window and door replacement services with Renewal, Plaintiff provided Defendant with her PII. Defendant used that PII to facilitate its services to Plaintiff and required Plaintiff to provide that PII to obtain window and door replacement services.

28. In collecting and maintaining customers' PII, Renewal implicitly agrees it will safeguard the data using reasonable means according to its internal policies, as well as state and federal law.

29. According to the Breach Notice, Renewal claims to have been "notified of a

[2] Andersen's Privacy Policy, https://www.andersenwindows.com/support/privacy/?_gl=1*1vmabeb*_ga*MTU2MTg0ODYxMS4xNjg3Mjg4ODk3*_ga_TYR3E13D05*MTY4NzI4ODg5Ni4xLjEuMTY4NzI4OTQwMS4wLjAuMA..&_ga=2.202791445.561460029.1687288897-1561848611.1687288897 (last visited June 20, 2023).

suspected data security event involving one of its systems" on January 19, 2023. Renewal further admits that an internal investigation revealed that "one of its systems was unsecured between January 2018 and January 19, 2023". Ex. A.

30. In other words, Defendant's investigation revealed that its network had been hacked by cybercriminals and that Defendant's inadequate cyber and data security systems and measures allowed those responsible for the cyberattack to obtain files containing a treasure trove of thousands of Renewal former and current customers' PII. Additionally, Defendant's investigation further revealed a complete failure by Renewal to recognize that parts of its systems had been unsecured and fully accessible to cybercriminals for *five years* before January 2023.

31. Additionally, Defendant admitted that PII may have been actually stolen during the Data Breach confessing that Renewal is "unable to rule out unauthorized access to, or taking of, personal information stored within the system". Ex. A.

32. On information and belief, Defendant was notified by Cybernews researchers in January 2023, that portions of its cloud storage containing around a million files, including nearly 300,000 documents with the PII former and current customers, was unprotected and fully accessible to the public. [3]

33. The types of PII accessible to the public included names, home addresses, contact details, and customer's physical signatures signature. The exposure of customers' signatures, Cybernews warns, was particularly concerning as cybercriminals are able to impersonate and sign documents on behalf of the individual. [4]

In addition to public access to former and current customers' PII, Cybernews researchers

[3] Andersen Corporation leaks customer home photos and address, Cybernews, https://cybernews.com/security/andersen-leak-home-photos-addresses/ (last visited June 20, 2023).
[4] *Id*.

also revealed that Renewal's unprotected cloud storage included photographs of customer homes dating back to at least 2016.

34. Cybernews warns that by allowing cybercriminals unfettered access to its cloud storage, Renewal was placing its customers' at risk not just for identity theft, fraud, and phishing scams, but also burglaries and threat actors impersonating its victims signatures and signing documents fraudulently. As a self-touted leader in its industry, Renewal knew or should have known of the tactics cybercriminals employ as well as the risks its unsecured cloud access presented to its customers.

> Cybernews researchers warn that such data leaks are dangerous, as threat actors can use personal information like names, emails, phone numbers, and addresses for phishing scams, identity theft, and other types of fraud.
>
> Details about the renovation work and pictures of the homes can make the victims more susceptible to burglaries. Additionally, leaked physical signatures in the form of hashes can allow threat actors to impersonate and sign documents on behalf of the individual.

35. Finally, Cybernews researchers warn that Renewal's failure to implement any authorization requirement to its cloud storage means that access by cybercriminals would technically be authorized by default, making it exceedingly difficult to identify details of a Breach including when it occurred, what was taken, and who it was perpetuated by.

36. Despite its duties and alleged commitments to safeguard PII, Renewal does not follow industry standard practices in securing former and current customers' PII, as evidenced by the Data Breach.

37. In response to the Data Breach, Renewal contends that it has "security measures in place to protect the security of information in our care, including security policies and procedures,

updated security configurations, advanced controls, and preventative scans" Ex. A. Although Renewal fails to expand on what these alleged "security policies and procedures" and "updated security configurations" are, such updates and security procedures should have been in place before the Data Breach.

38. Through its Breach Notice, Renewal also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity or errors." Ex. A.

39. On information and belief, Renewal has offered two years of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers.

40. Even with a year of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

41. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

42. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine this with

other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

43. On information and belief, Renewal failed to adequately train its IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its former and current customers' PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

Plaintiff's Experience

44. Plaintiff utilized Defendant's door replacement services between 2013 and 2014, when Renewal replaced a patio door at her home.

45. As a condition of utilizing Defendant's services, Ms. Anderson provided her PII to Renewal and trusted that the company would use reasonable measures to protect it according to Renewal's internal policies and state law.

46. Ms. Anderson reasonably believed that a portion of the funds she paid to Renewal for its services would be used for adequate cybersecurity protection for her PII.

47. Following the Data Breach, Ms. Anderson received an email from Intuit stating that her PII had been exposed in Renewal Data Breach.

48. Renewal deprived Plaintiff of the earliest opportunity to guard her PII against the Data Breach's effects by failing to notify her in a timely and prompt manner.

49. As a result of the Data Breach and the recommendation of Defendant's Notice Plaintiff has several hours of her time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, and self-monitoring her information to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

50. Ms. Anderson fears for her personal financial security and uncertainty over what PII exposed in the Data Breach. Ms. Anderson has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

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

52. Plaintiff has suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

53. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties and possibly criminals.

54. Indeed, Plaintiff began experiencing spam texts and phone calls following the Data Breach, suggesting her PII were in the hands of cybercriminals.

55. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

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

56. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

57. The ramifications of Defendant's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, date of birth, Social Security number, or driver's license

number, without permission, to commit fraud or other crimes.

58. The types of PII compromised and potentially stolen in the Data Breach is highly valuable to identity thieves. The customers' stolen PII can be used to gain access to a variety of existing accounts and websites to drain assets, bank accounts or open phony credit cards.

59. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover, Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

60. Identity thieves can also use the stolen data to harm Plaintiff and Class members through embarrassment, blackmail, or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and refunds, and obtaining government benefits. A Presidential Report on identity theft from 2008 states that:

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health- related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

61. As a result of Renewal's failure to prevent the Data Breach, Plaintiff and the

proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

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

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

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

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

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as defendant fails to undertake the appropriate measures to protect the PII in their possession.

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

63. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

64. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

65. One such example of criminals using PII for profit is the development of "Fullz" packages.

66. Cyber-criminals 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 in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

67. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. 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 members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

68. Defendant disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and members of the proposed Class 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.

69. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, as evidenced by its complete failure to prevent malware in its systems, demonstrates a willful and conscious disregard for privacy, and has exposed the PII of Plaintiff and the Class to unscrupulous operators, con-artists, and criminals.

70. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and the Class's 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.

Defendant failed to adhere to FTC guidelines.

71. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

72. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

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.

73. The guidelines also recommend that businesses watch for large amounts of data

being transmitted from the system and have a response plan ready in the event of a breach.

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

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

76. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to former and current customers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Fails to Comply with Industry Standards

77. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

78. Several best practices have been identified that a minimum should be implemented by employers in possession of PII, like Defendant, including but not limited to: 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. Defendant failed to follow

these industry best practices, including a failure to implement multi-factor authentication.

79. Other best cybersecurity practices that are standard for employers 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; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

80. Such cybersecurity practices are consistent with the advice provided by the cybernews researchers that first brought Renewal's unprotected cloud storage to its attention:

Data leak could have been prevented

According to the Cybernews research team, the cause of the leak was an unprotected Azure Storage blob. The leak could have been prevented by implementing proper authorization controls to block public access to cloud storage. Here are the ways how companies using an Azure Storage Blob can prevent data leaks:

- **Access control:** Azure Storage blobs support various access control mechanisms, such as Azure Active Directory authentication and Role-Based Access Control (RBAC). Using these tools can restrict access to the blob to only authorized users.
- **Network security:** Access to the blob should be limited to trusted internal networks only. Network security groups can be used to restrict access to the blob from specific IP addresses or virtual networks.
- **Encryption:** Azure Storage blobs support server-side encryption that encrypts the stored data and protects it if an unauthorized user accidentally gains access to the blob.
- **Auditing and logging:** Azure Storage blobs support auditing and logging, which helps to detect, track and investigate unauthorized access.
- **Regular review:** A company should regularly review the access control, network security, encryption, and auditing/logging settings to ensure they are still appropriate and effective.
- **Employee training:** Employee training on data security and handling sensitive information is essential to prevent human errors that can lead to data breaches.

81. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5,

PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

82. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

83. Plaintiff sues on behalf of herself and the proposed Class ("Class"), defined as follows:

> **All individuals in the United States whose PII was accessed without authorization in the Data Breach, including all those who received a notice of the Data Breach.**

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

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

86. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

87. **Numerosity**. Plaintiff is representative of the proposed Class, consisting of potentially thousands of members, far too many to join in a single action;

88. **Ascertainability**. Class members are readily identifiable from information in Defendant's possession, custody, and control;

89. **Typicality.** Plaintiff's claims are typical of Class member's claims as each arises

from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

90. **Adequacy.** Plaintiff will fairly and adequately protect the proposed Class's interests. Her interests does not conflict with Class members' interests, and she has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

91. **Commonality.** Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

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

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

c. Whether Defendant was negligent in maintaining, protecting, and securing PII;

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

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

f. Whether Defendant's Breach Notice was reasonable;

g. Whether the Data Breach caused Plaintiff's and the Class's injuries;

h. What the proper damages measure is; and

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

92. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

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

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

94. Plaintiff and members of the Class entrusted their PII to Renewal. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their PII and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendant's security systems to ensure the PII of Plaintiff and the Class was adequately secured and protected, including using encryption technologies. Defendant further had a duty to implement processes that would detect a breach of its security system in a timely manner.

95. Renewal was under a basic duty to act with reasonable care when it undertook to collect, create, and store Plaintiff's and the Class's PII on its computer system, fully aware–as any reasonable entity of its size would be–of the prevalence of data breaches and the resulting harm such a breach would cause. The recognition of Defendant's duty to act reasonably in this context is consistent with, *inter alia*, the Restatement (Second) of Torts § 302B (1965), which recounts a basic principle: an act or omission may be negligent if the actor realizes or should realize it involves an unreasonable risk of harm to another, even if the harm occurs through the criminal acts of a third party.

96. Defendant knew that the PII of Plaintiff and the Class was information that is valuable to identity thieves and other criminals. Defendant also knew of the serious harms that could happen if the PII of Plaintiff and the Class was wrongfully disclosed.

97. By being entrusted by Plaintiff and the Class to safeguard their PII, Defendant had a special relationship with Plaintiff and the Class. Plaintiff's and the Class's PII was provided to Renewal with the understanding that Defendant would take appropriate measures to protect it and would inform Plaintiff and the Class of any security concerns that might call for action by Plaintiff and the Class.

98. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information and allowing unauthorized access to Plaintiff's and the Class's PII.

99. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the Class, their PII would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the PII of Plaintiff and the Class and all resulting damages.

100. The injury and harm suffered by Plaintiff and the Class members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' PII.

101. As a result of Defendant's failure, the PII of Plaintiff and the Class were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII was disclosed to third parties without their consent. Plaintiff and Class members also suffered diminution in value of their PII in that it is now easily available to hackers on the Dark

Web. Plaintiff and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

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

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

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

105. Defendant violated its 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. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

106. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive

practices, caused the same harm as that suffered by Plaintiff and the Class.

107. Defendant had a duty to Plaintiff and the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and the Class's PII.

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

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

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

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

112. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

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

114. Entrust offered door and window replacement services to Plaintiff and members of

the Class in exchange for their PII.

115. In turn, and through internal policies, Renewal agreed they would not disclose the PII it collects to unauthorized persons. Renewal also promised to safeguard its customers' PII.

116. Plaintiff and the Class accepted Renewal offers by disclosing their PII to Renewal in exchange for its door and window services.

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

118. Plaintiff and the Class would not have entrusted their PII to Renewal in the absence of such an agreement with Renewal.

119. Renewal materially breached the contract(s) it had entered into with Plaintiff and the Class by failing to safeguard such information and failing to notify them promptly of the Data Breach that compromised such information. Renewal further breached the implied contracts with Plaintiff and the Class by:

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

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

c. Failing to ensure the confidentiality and integrity of PII that Renewal created, received, maintained, and transmitted.

120. The damages sustained by Plaintiff and the Class as described above were the direct and proximate result of Renewal's material breaches of their agreement(s).

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

122. The covenant of good faith and fair dealing is an element of every contract. All

such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

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

124. Renewal failed to advise Plaintiff and the Class of the Data Breach promptly and sufficiently.

125. In these and other ways, Renewal violated its duty of good faith and fair dealing.

126. Plaintiff and the Class have sustained damages because of Renewal's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

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

128. Plaintiff and Class members conferred a benefit upon Defendant. After all, Defendant benefitted from using their PII to provide door and window replacement services.

129. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class members. And Defendant benefited from receiving Plaintiff's and Class members' PII, as this was used to provide door and window services.

130. Plaintiff and Class members reasonably understood that Defendant would use

adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

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

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

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

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

135. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT V
Invasion of Privacy/Intrusion upon Seclusion
(On Behalf of Plaintiff and the Class)

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

137. Plaintiff and the Class had a legitimate expectation of privacy regarding their PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

138. Defendant owed a duty to Plaintiff and the Class to keep their PII confidential.

139. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of

Plaintiff's and the Class's PII is highly offensive to a reasonable person. Defendant's reckless and negligent failure to protect Plaintiff's and the Class's PII constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

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

141. Because Defendant failed to properly safeguard Plaintiff's and the Class's PII, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

142. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiff and the Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

143. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII is still maintained by Defendant with their inadequate cybersecurity system and policies.

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

145. Plaintiff, on behalf of herself and Class Members, seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' PII.

146. Plaintiff, on behalf of herself and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

PRAYER FOR RELIEF

147. Plaintiff and members of the Class demand a jury trial on all claims so triable and request 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 is necessary to protect the interests of Plaintiff and the Class;

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

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include 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 such other or further relief as may be appropriate under the circumstances.

JURY TRIAL DEMANDED

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

TURKE & STRAUSS LLP

DATED: June 21, 2023

By, */s/Raina C. Borrelli*

Raina C. Borrelli (MN No: 0392127)
raina@turkestrauss.com
Samuel J. Strauss (*pro hac vice forthcoming*)
sam@turkestrauss.com
613 Williamson St., Suite 201
Madison, WI 53703
Telephone (608) 237-1775
Facsimile: (608) 509-4423

Attorneys for Plaintiff and Proposed Class

ClassAction.org