UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

SEATTLE DIVISION

THOMAS VALENTINE, on behalf of himself and all others similarly situated, Plaintiff, v. **GREEN DIAMOND RESOURCE COMPANY,** Defendant.	Case No. 2:24-cv-620 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Thomas Valentine, ("Plaintiff"), individually and on behalf of all similarly situated persons, allege the following against Green Diamond Resource Company ("Green Diamond" or "Defendant") based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by Plaintiff's counsel and review of public documents as to all other matters:

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

I. INTRODUCTION

1. Plaintiff brings this class action against Green Diamond for its failure to properly secure and safeguard Plaintiff's and other similarly situated persons' name, date of birth, medical information, health insurance information, Social Security number, financial account information, driver's license number or state identification number, government-issued identification number, passport number, and full access credentials (the "Private Information") from hackers.

2. Green Diamond, based in Seattle, Washington, is a forest products company that owns and manages working forests in nine states throughout the western and southern U.S.

3. On or about April 19, 2024 Green Diamond filed official notice of a hacking incident with the Office of the Maine Attorney General. Under state law, organizations must report breaches involving medical information, health insurance information, Social Security number, financial account information, driver's license number or state identification number, government-issued identification number, passport number, and full access credentials.

4. On or around the same time, Green Diamond also sent out data breach letters to individuals whose information was compromised as a result of the hacking incident.

5. Based on the Notice filed by the company, Green Diamond detected unusual activity on some of its computer systems on June 27, 2023. In response, the company launched an investigation. The Green Diamond investigation revealed that an unauthorized party had access to certain company files between June 26 and June 27, 2023 (the "Data Breach"). Yet, Green Diamond waited until April 2024 to notify the public that they were at risk.

6. As a result of this delayed response, Plaintiff and "Class Members" (defined below) had no idea for almost a year that their Private Information had been compromised, and that they

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

7. The Private Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves, including but not limited to, medical information, health insurance information, Social Security number, financial account information, driver's license number or state identification number, government-issued identification number, passport number, and full access credentials that Green Diamond collected and maintained.

8. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, and obtaining driver's licenses in Class Members' names but with another person's photograph.

9. There has been no assurance offered by Green Diamond that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

10. Therefore, Plaintiff and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

11. Plaintiff brings this class action lawsuit to address Green Diamond's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and its failure to provide timely and adequate notice to Plaintiff and Class Members of the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

12. The potential for improper disclosure and theft of Plaintiff's and Class Members' Private Information was a known risk to Green Diamond, and thus Green Diamond was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

13. Plaintiff's and Class Members' identities are now at risk because of Green Diamond's negligent conduct as the Private Information that Green Diamond collected and maintained is now in the hands of data thieves and other unauthorized third parties.

14. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

15. Accordingly, Plaintiff, on behalf of himself and the Class, asserts claims for negligence, negligence *per se*, breach of implied contract, violations of the Washington Consumer Protection Act (RCW 19.86.020), unjust enrichment, and declaratory relief.

II. PARTIES

16. Plaintiff Thomas Valentine is, and at all times mentioned herein was, an individual citizen of the State of Washington.

17. Defendant Green Diamond is a forest products company incorporated in Washington State with its principal place of business at 1301 5th Avenue Suite 2700 in Seattle, Washington.

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

III. JURISDICTION AND VENUE

18. The 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. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Green Diamond. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

19. This Court has jurisdiction over Green Diamond because Green Diamond operates in and/or is incorporated in this District.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and Green Diamond has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. Green Diamond's Business and Collection of Plaintiff's and Class Members' Private Information

21. Green Diamond is a forest products company. Founded in 1890, Green Diamond is one of the five largest timberland owner-operator companies in the United States, serving customers in nine states. Green Diamond employs more than 375 people and generates approximately $76.7 million in annual revenue.

22. As a condition of receiving forest product services, Green Diamond requires that its customers entrust it with highly sensitive personal information. In the ordinary course of receiving service from Green Diamond, Plaintiff and Class Members were required to provide their Private Information to Defendant.

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

23. Green Diamond uses this information, *inter alia*, to maintain technical and functional updates of their website, advertising, and marketing.

24. In its privacy policy, Green Diamond promises its customers that it will not share this Private Information with third parties:

> "Under no circumstances will Green Diamond Resource Company sell personally identifying information to outside organizations, entities or companies without a user's consent."[1]

25. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Green Diamond assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

26. Plaintiff and Class Members relied on Green Diamond to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this information, which Defendant ultimately failed to do.

B. The Data Breach and Green Diamond's Inadequate Notice to Plaintiff and Class Members

27. According to Defendant's Notice, it learned of unauthorized access to its computer systems on June 27, 2023, with such unauthorized access having taken place between June 26 and June 27, 2023.

28. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including name, social security number, and date of birth.

[1] https://www.greendiamond.com/privacy-policy/ (last visited on May 6, 2024).

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

29. On or about April 19, 2024, roughly 10 months after Green Diamond learned that the Class's Private Information was first accessed by cybercriminals, Green Diamond finally began to notify customers that its investigation determined that their Private Information was accessed.

30. Green Diamond delivered Data Breach Notification Letters to Plaintiff and Class Members, alerting them that their highly sensitive Private Information had been exposed in a "Data Incident."

31. The notice letter then attached some pages entitled "Steps You Can Take to Protect Your Personal Information", which listed generic steps that victims of data security incidents can take, such as enrolling in monitoring services and monitoring accounts. Other than providing one year of crediting monitoring that Plaintiff and Class Members would have to affirmatively sign up for and a call center number that victims could contact "with any questions," Green Diamond offered no other substantive steps to help victims like Plaintiff and Class Members to protect themselves. On information and belief, Green Diamond sent a similar generic letter to all individuals affected by the Data Breach.

32. Green Diamond had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

33. Plaintiff and Class Members provided their Private Information to Green Diamond with the reasonable expectation and mutual understanding that Green Diamond would comply with its obligations to keep such information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

34. Green Diamond's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

35. Green Diamond knew or should have known that its electronic records would be targeted by cybercriminals.

C. Green Diamond Failed to Comply with FTC Guidelines

36. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

37. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

38. The FTC further recommends that companies not maintain personally identifiable information ("PII") longer than is needed for authorization of a transaction, limit access to sensitive

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

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

39. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by 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 the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

40. As evidenced by the Data Breach, Green Diamond failed to properly implement basic data security practices. Green Diamond's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

41. Green Diamond was at all times fully aware of its obligation to protect the Private Information of its customers yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

D. Green Diamond Failed to Comply with Industry Standards

42. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

43. Some industry best practices that should be implemented by businesses like Green Diamond include but are not limited to educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

44. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

45. 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.

46. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

E. Green Diamond Breached its Duty to Safeguard Plaintiff's and Class Members' Private Information

47. In addition to its obligations under federal and state laws, Green Diamond owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Green Diamond owed a duty to Plaintiff and Class Members to provide reasonable security, including complying with

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

industry standards and requirements, training for its staff, and ensuring that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

48. Green Diamond breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Green Diamond's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of its customers Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

49. Green Diamond negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

50. Had Green Diamond remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

51. Accordingly, Plaintiff's and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiff and Class Members also lost the benefit of the bargain they made with Green Diamond.

F. Green Diamond Should Have Known that Cybercriminals Target Private Information to Carry Out Fraud and Identity Theft

52. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[2] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

53. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity

[2] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on May 6, 2024).

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

54. Because a person's identity is akin to a puzzle, 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 otherwise harass or track the victim. 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 individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

55. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

56. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

57. One such example of this is the development of "Fullz" packages.

58. Cybercriminals can cross-reference two sources of the Private Information compromised in the Data Breach to marry unregulated data available elsewhere to criminally

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

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.

59. The development of "Fullz" packages means that the stolen Private Information 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 sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen 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 and other Class Members' stolen Private Information are being misused, and that such misuse is fairly traceable to the Data Breach.

60. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[3] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

61. Identity thieves can also use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud,

[3] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited May 6, 2024).

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

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

62. PII is data that can be used to detect a specific individual. PII is a valuable property right. Its value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts (which include heavy prison sentences). Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has considerable market value.

63. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[4] The increase in cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry.

64. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[5] Experian reports that a stolen credit or debit card number can

[4] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. Dep't of Justice, Feb. 10, 2020, available at https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-fourmembers-china-s-military (last visited on May 6, 2024).

[5] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited on May 6, 2024).

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

sell for $5 to $110 on the dark web and that the "*fullz*" (a term criminals who steal credit card information use to refer to a complete set of information on a fraud victim) sold for $30 in 2017.[6]

65. Furthermore, even information such as names, email addresses and phone numbers, can have value to a hacker. Beyond things like spamming customers, or launching phishing attacks using their names and emails, hackers, *inter alia*, can combine this information with other hacked data to build a more complete picture of an individual. It is often this type of piecing together of a puzzle that allows hackers to successfully carry out phishing attacks or social engineering attacks. This is reflected in recent reports, which warn that "[e]mail addresses are extremely valuable to threat actors who use them as part of their threat campaigns to compromise accounts and send phishing emails."[7]

66. The Dark Web Price Index of 2022, published by PrivacyAffairs[8] shows how valuable just email addresses alone can be, even when not associated with a financial account:

Email Database Dumps	**Avg. Price USD (2022)**
10,000,000 USA email addresses	$120
600,000 New Zealand email addresses	$110
2,400,000 million Canada email addresses	$100

[6] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited on May 6, 2024).

[7] *See* https://www.magicspam.com/blog/dark-web-price-index-the-cost-of-email-data/ (last visited on May 6, 2024).

[8] *See* https://www.privacyaffairs.com/dark-web-price-index-2022/ (last visited on May 6, 2024).

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

67. Beyond using email addresses for hacking, the sale of a batch of illegally obtained email addresses can lead to increased spam emails. If an email address is swamped with spam, that address may become cumbersome or impossible to use, making it less valuable to its owner.

68. Likewise, the value of PII is increasingly evident in our digital economy. Many companies including Green Diamond collect PII for purposes of data analytics and marketing. These companies, collect it to better target customers, and shares it with third parties for similar purposes.[9]

69. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[10]

70. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not only by a price at which consumers or hackers actually seek to sell it, but rather by the economic benefit consumers derive from being able to use it and control the use of it.

71. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value of the PII.

---

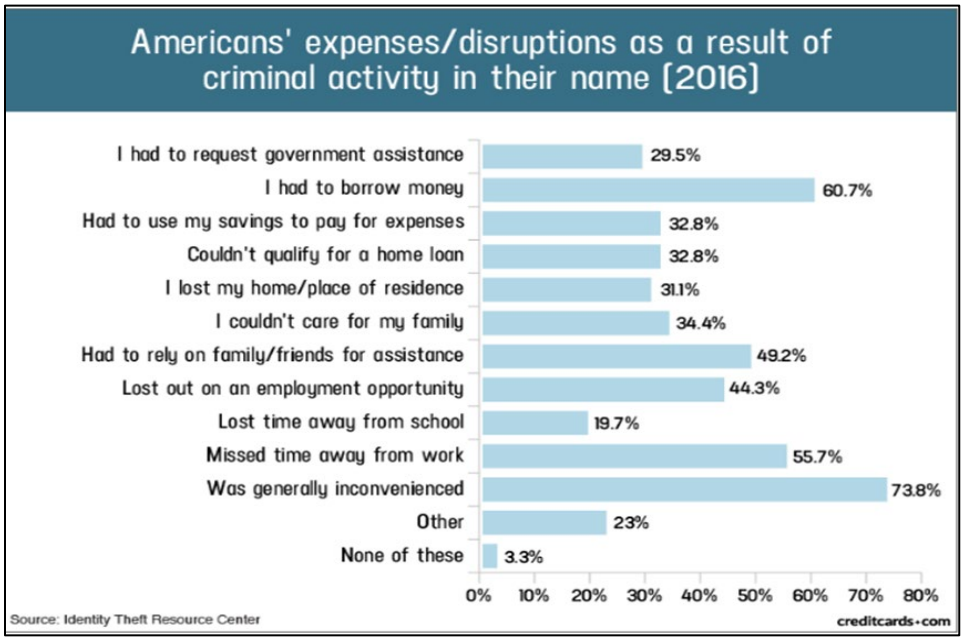
[9] *See* https://robinhood.com/us/en/support/articles/privacy-policy/ (last visited on May 6, 2024).

[10] *See* John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets,* 15 Rich. J. L. & Tech. 11, 14 (2009).

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

72. Data breaches, like that at issue here, damage consumers by interfering with their fiscal autonomy. Any past and potential future misuse of Plaintiff's PII impairs their ability to participate in the economic marketplace.

73. A study by the Identity Theft Resource Center[11] shows the multitude of harms caused by fraudulent use of PII:



74. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or personal financial information

[11] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited May 6, 2024).

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[12]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

75. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

76. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

G. Plaintiff's and Class Members' Damages

Plaintiff Valentine's Experience

77. Plaintiff Valentine is a former customer of Green Diamond.

78. When Plaintiff first became a customer, Defendant required Plaintiff Valentine provide it with substantial amounts of his PII.

79. On or about April 19, 2024, Plaintiff Valentine received a letter entitled "Notice of Security Incident" which told him that his Private Information had been accessed during the Data Breach. The notice letter informed him that the Private Information compromised included his "name, Social Security Number, and date of birth."

[12] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited May 6, 2024).

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

80. The notice letter offered Plaintiff Valentine only 1 year of credit monitoring services. 1 year of credit monitoring is not sufficient given that Plaintiff Valentine will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of her Private Information.

81. Plaintiff Valentine suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring his accounts for fraud.

82. Plaintiff Valentine would not have provided his Private Information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its customers' personal information from theft, and that those systems were subject to a data breach.

83. Plaintiff Valentine suffered actual injury in the form of having his Private Information compromised and/or stolen as a result of the Data Breach.

84. Plaintiff Valentine suffered actual injury in the form of damages to and diminution in the value of his personal information – a form of intangible property that Plaintiff Valentine entrusted to Defendant for the purpose of receiving forest product services from Defendant and which was compromised in, and as a result of, the Data Breach.

85. Plaintiff Valentine suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Private Information being placed in the hands of criminals.

86. Plaintiff Valentine has a continuing interest in ensuring that his Private Information, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

87. As a result of the Data Breach, Plaintiff Valentine made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant, as well as long-term credit monitoring options he will now need to use. Plaintiff Valentine has spent several hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

88. As a result of the Data Breach, Plaintiff Valentine has suffered anxiety as a result of the release of his Private Information to cybercriminals, which Private Information he believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of committing cyber and other crimes against him. Plaintiff Valentine is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on his life.

89. Plaintiff Valentine also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff Valentine; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud he now faces.

90. As a result of the Data Breach, Plaintiff Valentine anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

91. In sum, Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

92. Plaintiff and Class Members entrusted their Private Information to Defendant in order to receive Defendant's services.

93. Plaintiff's Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices.

94. As a direct and proximate result of Green Diamond's actions and omissions, Plaintiff and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

95. Further, as a direct and proximate result of Green Diamond's conduct, Plaintiff and Class Members have been forced to spend time dealing with the effects of the Data Breach.

96. Plaintiff and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiff and Class Members.

97. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiff and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiff and Class Members.

98. Plaintiff and Class Members also lost the benefit of the bargain they made with Green Diamond. Plaintiff and Class Members overpaid for services that were intended to be accompanied by adequate data security but were not. Indeed, part of the price Plaintiff and Class

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

Members paid to Green Diamond was intended to be used by Green Diamond to fund adequate security of Green Diamond's system and protect Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class did not receive what they paid for.

99. Additionally, as a direct and proximate result of Green Diamond's conduct, Plaintiff and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

100. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

101. Additionally, Plaintiff and Class Members also suffered a loss of value of their PII and PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[13] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[14]

[13] *See* https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/#:~:text=The%20business%20of%20data%20brokering,annual%20revenue%20of%20%24200%20billion. (last visited on May 6, 2024).

[14] *Frequently Asked Questions,* Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited May 6, 2024).

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

102. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiff and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiff and the Class Members, thereby causing additional loss of value.

103. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. The contractual bargain entered into between Plaintiff and Green Diamond included Defendant's contractual obligation to provide adequate data security, which Defendant failed to provide. Thus, Plaintiff and Class Members did not get what they bargained for.

104. Finally, Plaintiff and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses include, but are not limited to, the following:

a. Monitoring for and discovering fraudulent accounts;

b. Spending time on the phone with or at a financial institution to dispute fraudulent accounts;

c. Contacting financial institutions and closing or modifying financial accounts; and

d. Closely reviewing and monitoring bank accounts and credit reports for additional unauthorized activity for years to come.

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

105. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Green Diamond, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

106. As a direct and proximate result of Green Diamond's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

107. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

108. Specifically, Plaintiff proposes the following Nationwide Class, as well as the following Washington Subclass definitions (also collectively referred to herein as the "Class"), subject to amendment as appropriate:

Nationwide Class

All individuals in the United States who had Private Information accessed as a result of the Data Breach, including all who were sent a notice of the Data Breach.

Washington Subclass

All residents of Washington State who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

109. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

110. Plaintiff reserves the right to modify or amend the definitions of the proposed Nationwide Class, as well as the Washington Subclass before the Court determines whether certification is appropriate.

111. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

112. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of 27,896 persons associated with Green Diamond whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Green Diamond's records, Class Members' records, publication notice, self-identification, and other means.

113. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Green Diamond engaged in the conduct alleged herein;

b. Whether Green Diamond's conduct violated the Washington Consumer Protection Act invoked below;

c. When Green Diamond learned of the Data Breach;

d. Whether Green Diamond's response to the Data Breach was adequate;

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

e. Whether Green Diamond unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

f. Whether Green Diamond failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

g. Whether Green Diamond's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Green Diamond's data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Green Diamond owed a duty to Class Members to safeguard their Private Information;

j. Whether Green Diamond breached its duty to Class Members to safeguard their Private Information;

k. Whether hackers obtained Class Members' Private Information via the Data Breach;

l. Whether Green Diamond had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;

m. Whether Green Diamond breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

n. Whether Green Diamond knew or should have known that its data security systems and monitoring processes were deficient;

o. What damages Plaintiff and Class Members suffered as a result of Green Diamond's misconduct;

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

p. Whether Green Diamond's conduct was negligent;

q. Whether Green Diamond's conduct was *per se* negligent;

r. Whether Green Diamond was unjustly enriched;

s. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

t. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

u. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

114. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

115. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

116. Predominance. Green Diamond has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Green Diamond's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

117. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Green Diamond. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

118. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Green Diamond has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

119. Finally, all members of the proposed Class are readily ascertainable. Green Diamond has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Green Diamond.

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE WASHINGTON SUBCLASS)

120. Plaintiff restates and realleges all of the allegations stated above and hereafter as if fully set forth herein.

121. Green Diamond knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

122. Green Diamond's duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

123. Green Diamond knew or should have known of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate security. Green Diamond was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

124. Green Diamond owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to it. Green Diamond's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

b. To protect customers' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to the FTCA and the Washington Consumer Protection Act.

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiff and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

125. Green Diamond's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

126. Green Diamond's duty also arose because Defendant was bound by industry standards to protect its customers' confidential Private Information.

127. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and Green Diamond owed them a duty of care to not subject them to an unreasonable risk of harm.

128. Green Diamond, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

safeguarding Plaintiff's and Class Members' Private Information within Green Diamond's possession.

129. Green Diamond, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

130. Green Diamond, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

131. Green Diamond breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

132. Green Diamond acted with reckless disregard for the rights of Plaintiff and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiff and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

133. Green Diamond had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust Green Diamond with their Private Information was predicated on the understanding that Green Diamond would take adequate security precautions. Moreover, only Green Diamond had the ability to protect its systems (and the Private Information that it stored on them) from attack.

134. Green Diamond's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised, and exfiltrated as alleged herein.

135. Green Diamond's breaches of duty also caused a substantial, imminent risk to Plaintiff and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

136. As a result of Green Diamond's negligence in breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

137. Green Diamond also had independent duties under state laws that required it to reasonably safeguard Plaintiff's and Class Members' Private Information and promptly notify them about the Data Breach.

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

138. As a direct and proximate result of Green Diamond's negligent conduct, Plaintiff and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

139. The injury and harm that Plaintiff and Class Members suffered was reasonably foreseeable.

140. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

141. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Green Diamond to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On behalf of Plaintiff and the Nationwide Class or Alternatively the Washington Subclass)

142. Plaintiff restates and realleges the allegations in paragraphs of the proceeding factual allegations above as if fully set forth herein.

143. Pursuant to Section 5 of the FTCA, Green Diamond had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiff and Class Members.

144. Green Diamond breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

145. Plaintiff and Class Members are within the class of persons that the FTCA is intended to protect.

146. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of Green Diamond's duty in this regard.

147. Green Diamond violated the FTCA by failing to use reasonable measures to protect the Private Information of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

148. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Green Diamond's networks, databases, and computers that stored Plaintiff's and Class Members' unencrypted Private Information.

149. Green Diamond's violations of the FTCA constitute negligence *per se*.

150. Plaintiff's and Class Members' Private Information constitutes personal property that was stolen due to Green Diamond's negligence, resulting in harm, injury, and damages to Plaintiff and Class Members.

151. As a direct and proximate result of Green Diamond's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

152. Green Diamond breached its duties to Plaintiff and the Class under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

153. As a direct and proximate result of Green Diamond's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

154. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Green Diamond to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Nationwide Class or Alternatively the Washington Subclass)

155. Plaintiff restates and realleges the allegations in the preceding factual allegations as if fully set forth herein.

156. Green Diamond provides forest product services to Plaintiff and Class Members. Plaintiff and Class Members formed an implied contract with Defendant regarding the provision of those services through their collective conduct, including by Plaintiff and Class Members paying for goods and services from Defendant.

157. Through Defendant's sale of goods and services, it knew or should have known that it must protect Plaintiff's and Class Members' confidential Private Information in accordance with Green Diamond's policies, practices, and applicable law.

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

158. As consideration, Plaintiff and Class Members paid money to Green Diamond and turned over valuable Private Information to Green Diamond. Accordingly, Plaintiff and Class Members bargained with Green Diamond to securely maintain and store their Private Information.

159. Green Diamond accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing goods and services to Plaintiff and Class Members.

160. In delivering their Private Information to Green Diamond and paying for goods and services, Plaintiff and Class Members intended and understood that Green Diamond would adequately safeguard the Private Information as part of that service.

161. Defendant's implied promises to Plaintiff and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

162. Plaintiff and Class Members would not have entrusted their Private Information to Green Diamond in the absence of such an implied contract.

163. Had Green Diamond disclosed to Plaintiff and the Class that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and Class Members would not have provided their Private Information to Green Diamond.

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

164. Green Diamond recognized that Plaintiff's and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

165. Green Diamond violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class Members' Private Information.

166. Plaintiff and Class Members have been damaged by Green Diamond's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT V
VIOLATION OF WASHINGTON CONSUMER PROTECTION ACT
(On behalf of Plaintiff and the Nationwide Class or Alternatively the Washington Subclass)

167. Plaintiff restates and realleges the allegations in the preceding factual allegations as if fully set forth herein.

168. As fully alleged above, Green Diamond engaged in unfair and deceptive acts and practices in violation of the Washington Consumer Protection Act.

169. The Washington State Consumer Protection Act, RCW 19.86.020 (the "WCPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described in the WCPA and relevant case law.

170. Defendant is a "person" as described in RWC 19.86.010(1).

171. Defendant engages in "trade" and "commerce" as described in RWC 19.86.010(2) in that it engages in the sale of services and commerce directly and indirectly affecting the people of the state of Washington.

172. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

unlawful, unfair and fraudulent practices within the meaning, and in violation of, the WCPA, in that Defendant's practices were injurious to the public interest because they injured other persons and have the capacity to injure other persons.

173. In the course of conducting business, Defendant committed "unfair or deceptive acts or practices" by *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII, and violating the common law alleged herein in the process. Plaintiff and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. As described above, Defendant's wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

174. Defendant also violated the WCPA by failing to time notify and concealing from Plaintiff and Class Members information regarding the unauthorized release and disclosure of their PII. If Plaintiff and Class Members had been notified in an appropriate manner, and had the information not been hidden from them, that could have taken precautions to safeguard and protect their PII and identities.

175. The seriousness of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

176. Reasonable individuals would be misled by Green Diamond's misrepresentations and/or omissions concerning the security of their Private Information because they assume companies, like Green Diamond, that collect PII from customers will properly safeguard such in a manner consistent with industry standards and practices.

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

177. Green Diamond failed to inform Plaintiff or Class Members of its inadequate data security practices and procedures that led to the Data Breach, thereby misleading Plaintiff and Class Members, in violation of RCW 19.86.020 *et seq*. Such misrepresentations and/or omissions were material because Plaintiff and Class Members entrusted Green Diamond with their Private Information.

178. Had Plaintiff and Class Members known of Green Diamond's failure to maintain adequate security measures to protect their Private Information, they would not have entrusted their Private Information to Defendant.

179. Plaintiff and Class Members were injured because: a) they would not have paid for services from Green Diamond had they known the true nature and character of Green Diamond's data security practices; b) Plaintiff and Class Members would not have entrusted their Private Information to Green Diamond in the absence of promises that Green Diamond would keep their information reasonably secure, and c) Plaintiff and Class Members would not have entrusted their Private Information to Green Diamond in the absence of the promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

180. As a result, Plaintiff and the Class Members have been damaged in an amount to be proven at trial.

181. On behalf of himself and other members of the Class, Plaintiff seeks to enjoin the unlawful acts and practices described herein, to recover actual damages, and reasonable attorneys' fees.

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

COUNT VI
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Nationwide Class or Alternatively the Washington State Subclass)

182. Plaintiff restates and realleges the allegations in all preceding factual allegations as if fully set forth herein.

183. This Count is pleaded in the alternative to Counts III above.

184. Plaintiff and Class Members conferred a benefit on Green Diamond by turning over their Private Information to Defendant and by paying for products and services that should have included cybersecurity protection to protect their Private Information. Plaintiff and Class Members did not receive such protection.

185. Upon information and belief, Green Diamond funds its data security measures entirely from its general revenue, including from payments made to it by Plaintiff and Class Members.

186. As such, a portion of the payments made by Plaintiff and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Green Diamond.

187. Green Diamond has retained the benefits of its unlawful conduct, including the amounts of payment received from Plaintiff and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

188. Green Diamond knew that Plaintiff and Class Members conferred a benefit upon it, which Green Diamond accepted. Green Diamond profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes, while failing to use the

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

payments it received for adequate data security measures that would have secured Plaintiff's and Class Members' Private Information and prevented the Data Breach.

189. If Plaintiff and Class Members had known that Green Diamond had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

190. Due to Green Diamond's conduct alleged herein, it would be unjust and inequitable under the circumstances for Green Diamond to be permitted to retain the benefit of its wrongful conduct.

191. As a direct and proximate result of Green Diamond's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity to control how their Private Information is used; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity 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; (v) the continued risk to their Private Information, which remains in Green Diamond's possession and is subject to further unauthorized disclosures so long as Green Diamond fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

192. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Green Diamond and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Green Diamond from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

193. Plaintiff and Class Members may not have an adequate remedy at law against Green Diamond, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VIII
DECLARATORY JUDGMENT
(On behalf of Plaintiff and the Nationwide Class or Alternatively the Washington Subclass)

194. Plaintiff restates and realleges the allegations in all preceding factual allegations as if fully set forth herein.

195. 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. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and state statute described in this Complaint.

196. Green Diamond owes a duty of care to Plaintiff and Class Members, which required it to adequately secure Plaintiff's and Class Members' Private Information.

197. Green Diamond still possesses Private Information regarding Plaintiff and Class Members.

198. Plaintiff alleges that Green Diamond's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his Private

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

Information and the risk remains that further compromises of his Private Information will occur in the future.

199. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Green Diamond owes a legal duty to secure its customers' Private Information and to timely notify customers of a data breach under the common law and Section 5 of the FTCA;

b. Green Diamond's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect customers' Private Information; and

c. Green Diamond continues to breach this legal duty by failing to employ reasonable measures to secure customers' Private Information.

200. This Court should also issue corresponding prospective injunctive relief requiring Green Diamond to employ adequate security protocols consistent with legal and industry standards to protect customers' Private Information, including the following:

a. Order Green Diamond to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Green Diamond must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks,

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

penetration tests, and audits on Green Diamond's systems on a periodic basis, and ordering Green Diamond to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Green Diamond's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating its users about the threats they face with regard to the security of their Private Information, as well as the steps Green Diamond's customers should take to protect themselves.

201. If an injunction is not issued, Plaintiff will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Green Diamond. The risk of another such breach is real, immediate, and substantial. If another breach at Green Diamond occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

202. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Green Diamond if an injunction is issued. Plaintiff will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Green Diamond's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Green Diamond has a pre-existing legal obligation to employ such measures.

203. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Green Diamond, thus preventing future injury to Plaintiff and other customers whose Private Information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Classes described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Nationwide Class and Washington Subclass requested herein;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
TEL. 872.263.1100 • FAX 872.263.1109
www.straussborrelli.com

d. An order instructing Green Diamond to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring Green Diamond to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: May 6, 2024

Respectfully submitted,

s/*Samuel J. Strauss*
Samuel J. Strauss, WSBA #46971
STRAUSS BORRELLI PLLC
980 N. Michigan Ave., Suite 1610
Chicago, Illinois 60611
Tel: 872-263-1100
sam@straussborrelli.com

Mason A. Barney
Tyler J. Bean
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: mbarney@sirillp.com
E: tbean@sirillp.com

ClassAction.org