



LAW GROUP, PLLC

7508 North 59th Avenue
Glendale, Arizona 85301
Telephone: (602) 730-7100
Fax: (602) 794-6956

Cristina Perez Hesano (#027023)
cperez@perezlawgroup.com
Attorney for Plaintiff & Class

Gary M. Klinger*
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com
**Pro Hac Vice Forthcoming*

Attorneys for Plaintiff and the Class

UNITED STATES DISTRICT COURT

DISTRICT OF ARIZONA

Maria Barrios, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

Farmers Investment Co. d/b/a Green
Valley Pecan Company, an Arizona
corporation,

Defendant.

Case No. _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

P
PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

1 Plaintiff Maria Barrios (“Plaintiff”) brings this Class Action Complaint (“Complaint”)
2 against Defendant Farmers Investment Co. d/b/a Green Valley Pecan Company (“Defendant”
3 or “Green Valley”) as an individual and on behalf of all others similarly situated, and alleges,
4 upon personal knowledge as to her own actions and her counsels’ investigation, and upon
5 information and belief as to all other matters, as follows:
6

7 **I. PARTIES**

8 1. Plaintiff Maria Barrios is a natural person, resident, and a citizen of the State of
9 Nevada, currently residing in Las Vegas. She has no intention of moving to a different state in
10 the immediate future. Plaintiff Barrios is acting on her own behalf and on behalf of others
11 similarly situated.
12

13 2. Defendant obtained and continues to maintain Plaintiff Barrios’ PII and thus
14 owed her a legal duty and obligation to protect that PII from unauthorized access and disclosure.
15

16 3. Plaintiff Barrios would not have entrusted her PII to Defendant had she known
17 that Defendant failed to maintain adequate data security.

18 4. Plaintiff Barrios’ PII was compromised and disclosed as a result of Defendant’s
19 inadequate data security, which resulted in the Data Breach.
20

21 5. Plaintiff received a notice letter from Defendant, via U.S. mail, dated January 12,
22 2023, informing her that the information compromised in the Data Breach included her name,
23 date of birth, and Social Security number.

24 6. Defendant is an Arizona-based retail company that sells pecans, among other
25 products, to its employees. Defendant’s principal place of business is located at 1525 E.
26 Sahuarita Road, Sahuarita, Arizona 85629.
27

P
PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

1 7. The true names and capacities of persons or entities, whether individual,
2 corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein
3 are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to
4 reflect the true names and capacities of such other responsible parties when their identities
5 become known.
6

7 8. All of Plaintiff’s claims stated herein are asserted against Defendant and any of
8 its owners, predecessors, successors, subsidiaries, agents and/or assigns.
9

10 **II. JURISDICTION AND VENUE**

11 9. This Court has subject matter jurisdiction over this action under 28 U.S.C. §
12 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or
13 value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the
14 proposed class, and at least one member of the class is a citizen of a state different from
15 Defendant.¹
16

17 10. This Court has personal jurisdiction over Defendant because its principal place
18 of business is in this District, the acts and omissions giving rise to Plaintiff’s claims occurred
19 in and emanated from this District, regularly conducts business in Arizona, and has sufficient
20 minimum contacts in Arizona.
21

22 11. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant’s principal place
23 of business is in this District and a substantial part of the events, acts, and omissions giving rise
24

25
26 ¹ According to the Office of Maine’s Attorney General, 10 Maine residents were impacted in
27 the Data Breach. See <https://apps.web.maine.gov/online/aewiewer/ME/40/176917d7-3364-41bd-9b16-80e11da3f497.shtml>



1 to Plaintiff’s claim occurred in this district.

2 **III. NATURE OF THE ACTION**

3 12. This class action arises out of the recent data breach (“Data Breach”) involving
4 Defendant, an Arizona-based retail company that claims it “produces some of the finest pecans
5 in the world[.]”¹
6

7 13. Plaintiff brings this Complaint against Defendant for its failure to properly secure
8 and safeguard the personally identifiable information that it collected and maintained as part of
9 its regular business practices, including, but not limited to, names, dates of birth, and Social
10 Security numbers, (collectively defined herein as “PII”).
11

12 14. Upon information and belief, current and former Green Valley employees are
13 required to entrust Defendant with sensitive, non-public PII, without which Defendant could
14 not perform its regular business activities, in order to obtain employment or certain employment
15 benefits at Defendant. Defendant retains this information for at least many years and even after
16 the employee-employer relationship has ended.
17

18 15. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff
19 and Class Members, Defendant assumed legal and equitable duties to those individuals to
20 protect and safeguard that information from unauthorized access and intrusion.
21

22 16. On or about May 31, 2022, Defendant “experienced a network disruption.”²
23 Defendant subsequently investigated the network disruption, and as a result of its investigation,
24

25
26 ¹ <https://www.greenvalleypecan.com/about-us/>

27 ² The “Notice Letter”. A sample copy is available at <https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-798.pdf>



1 Defendant concluded on August 26, 2022 that “personal information may have been accessed
2 or acquired by an unauthorized individual” during the Data Breach.¹

3 17. According to Defendant’s Notice of Data Security Incident letter (the “Notice
4 Letter”), the compromised PII included individuals’ names, dates of birth, and Social Security
5 numbers.²

6
7 18. Defendant’s investigation concluded that the PII compromised in the Data Breach
8 included Plaintiff’s and approximately 9,000 other individuals’ information.³

9
10 19. Defendant failed to adequately protect Plaintiff’s and Class Members PII—and
11 failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted
12 PII was compromised due to Defendant’s negligent and/or careless acts and omissions and its
13 utter failure to protect employees’ sensitive data. Hackers targeted and obtained Plaintiff’s and
14 Class Members’ PII because of its value in exploiting and stealing the identities of Plaintiff and
15 Class Members. The present and continuing risk of identity theft and fraud to victims of the
16 Data Breach will remain for their respective lifetimes.

17
18 20. Moreover, after the Data Breach, Defendant waited *over six months* (from May
19 31, 2022, to January 12, 2023) to notify Plaintiff and Class Members of the Data Breach and/or
20 inform them that their PII was compromised. During this time, Plaintiff and Class Members
21 were unaware that their sensitive PII had been compromised, and that they were, and continue
22

23
24
25

¹ *Id.*

26 ² *Id.*

27 ³ <https://apps.web.maine.gov/online/aeviewer/ME/40/176917d7-3364-41bd-9b16-80e11da3f497.shtml>

1 to be, at significant risk of identity theft and various other forms of personal, social, and
2 financial harm.

3 21. In breaching its duties to properly safeguard employees' PII and give employees
4 timely, adequate notice of the Data Breach's occurrence, Defendant's conduct amounts to
5 negligence and/or recklessness and violates federal and state statutes.
6

7 22. Plaintiff brings this action on behalf of all persons whose PII was compromised
8 as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class
9 Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information
10 security practices; and (iii) effectively secure hardware containing protected PII using
11 reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's
12 conduct amounts at least to negligence and violates federal and state statutes.
13

14 23. Defendant disregarded the rights of Plaintiff and Class Members by intentionally,
15 willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable
16 measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take
17 available steps to prevent an unauthorized disclosure of data, and failing to follow applicable,
18 required, and appropriate protocols, policies, and procedures regarding the encryption of data,
19 even for internal use. As a result, the PII of Plaintiff and Class Members was compromised
20 through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members
21 have a continuing interest in ensuring that their information is and remains safe, and they should
22 be entitled to injunctive and other equitable relief.
23
24

25 24. Plaintiff and Class Members have suffered injury as a result of Defendant's
26 conduct. These injuries include: (i) lost or diminished value of PII; (ii) lost opportunity costs
27

P
PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

1 associated with attempting to mitigate the actual consequences of the Data Breach, including
2 but not limited to lost time, (iii) invasion of privacy; and (iv) the continued and certainly
3 increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third
4 parties to access and abuse; and (b) remains backed up in Defendant’s possession and is subject
5 to further unauthorized disclosures so long as Defendant fails to undertake appropriate and
6 adequate measures to protect the PII.
7

8 25. Plaintiff seeks to remedy these harms and prevent any future data compromise on
9 behalf of herself and all similarly situated persons whose personal data was compromised and
10 stolen as a result of the Data Breach and who remain at risk due to Defendant’s inadequate data
11 security practices.
12

13 **IV. STATEMENT OF FACTS**

14 **A. Defendant’s Business.**

15 26. Defendant is an Arizona-based retail company that claims to sell “some of the
16 finest pecans in the world,” among other products and services.¹
17

18 27. Plaintiff and Class Members are current and former employees at Defendant.
19

20 28. In order to apply to be an employee or obtain certain employment-related benefits
21 at Defendant, Plaintiff and Class Members were required to provide sensitive and confidential
22 PII, including their names, dates of birth, Social Security numbers, driver’s license numbers,
23 financial information, and other sensitive information.
24
25
26

27 ¹ <https://www.greenvalleypecan.com/about-us/>



1 29. The information held by Defendant in its computer systems at the time of the
2 Data Breach included the unencrypted PII of Plaintiff and Class Members.

3 30. Upon information and belief, Defendant made promises and representations to its
4 employees, including Plaintiff and Class Members, that the PII collected from them as a
5 condition of their employment would be kept safe, confidential, that the privacy of that
6 information would be maintained, and that Defendant would delete any sensitive information
7 after it was no longer required to maintain it.
8

9 31. Plaintiff and Class Members provided their PII to Defendant with the reasonable
10 expectation and on the mutual understanding that Defendant would comply with its obligations
11 to keep such information confidential and secure from unauthorized access.
12

13 32. Plaintiff and Class Members have taken reasonable steps to maintain the
14 confidentiality of their PII. Plaintiff and Class Members relied on the sophistication of
15 Defendant to keep their PII confidential and securely maintained, to use this information for
16 necessary purposes only, and to make only authorized disclosures of this information. Plaintiff
17 and Class Members value the confidentiality of their PII and demand security to safeguard their
18 PII.
19

20 33. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff
21 and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to
22 keep its employees' PII safe and confidential.
23

24 34. Defendant had obligations created by FTC Act, contract, industry standards, and
25 representations made to Plaintiff and Class Members, to keep their PII confidential and to
26 protect it from unauthorized access and disclosure.
27

P
PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

1 35. Defendant derived a substantial economic benefit from collecting Plaintiff’s and
2 Class Members’ PII. Without the required submission of PII, Defendant could not perform the
3 services it provides.

4 36. By obtaining, collecting, using, and deriving a benefit from Plaintiff’s and Class
5 Members’ PII, Defendant assumed legal and equitable duties and knew or should have known
6 that it was responsible for protecting Plaintiff’s and Class Members’ PII from disclosure.
7

8 **B. The Data Breach.**

9 37. On or about January 12, 2023, Defendant began sending Plaintiff and other
10 victims of the Data Breach a Notice of Data Security Incident letter, informing them that:
11

12 **What Happened.** On or around May 31, 2022, FICO experienced a network disruption.
13 In response, we immediately took steps to secure our digital environment and engaged
14 a leading cybersecurity firm to assist with an investigation and determine whether
15 sensitive or personal information may have been accessed or acquired during the
16 incident. Through the investigation, on August 26, 2022, we found that personal
17 information may have been accessed or acquired by an unauthorized individual.
18 Following this confirmation, we engaged a vendor to conduct a thorough and extensive
19 review of potentially affected files to determine what personal information may have
20 been involved. Additionally, we began the process of locating mailing information and
21 setting up services being offered, which was completed on January 3, 2023.

22 ...

23 **What Information Was Involved.** The potentially affected information may have
24 included your Name, Date of Birth, and Social Security Number.

25 **What We Are Doing.** As soon as we discovered this incident, we took the steps
26 described above. As part of the response
27 process, we implemented additional measures to reduce the risk of a similar incident
occurring in the future. We have also reported the incident to the Federal Bureau of
Investigation and will cooperate with any resulting investigation.¹

¹¹ Notice Letter.



1 38. Omitted from the Notice Letter were the details of the root cause of the Data
2 Breach, the vulnerabilities exploited, why it took over six months from the day of the Data
3 Breach to inform impacted individuals that their information was involved, and the remedial
4 measures undertaken to ensure such a breach does not occur again. To date, these critical facts
5 have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest
6 in ensuring that their PII remains protected.
7

8 39. This “disclosure” amounts to no real disclosure at all, as it fails to inform, with
9 any degree of specificity, Plaintiff and Class Members of the Data Breach’s critical facts.
10 Without these details, Plaintiff’s and Class Members’ ability to mitigate the harms resulting
11 from the Data Breach is severely diminished.
12

13 40. Defendant did not use reasonable security procedures and practices appropriate
14 to the nature of the sensitive information they were maintaining for Plaintiff and Class
15 Members, causing the exposure of PII, such as encrypting the information or deleting it when
16 it is no longer needed.
17

18 41. The attacker targeted, accessed, and acquired files in Defendant’s computer
19 systems containing unencrypted PII of Plaintiff and Class Members, including their names,
20 dates of birth, and Social Security numbers. Plaintiff’s and Class Members’ PII was accessed
21 and stolen in the Data Breach.
22

23 42. Plaintiff further believes her PII, and that of Class Members, was subsequently
24 sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals
25 that commit cyber-attacks of this type.
26

27 **C. Data Breaches Are Preventable.**

P
PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

1 43. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could
2 and should have implemented, as recommended by the United States Government, the
3 following measures:

- 4 ● Implement an awareness and training program. Because end users are targets,
5 employees and individuals should be aware of the threat of ransomware and how it is
6 delivered.
- 7 ● Enable strong spam filters to prevent phishing emails from reaching the end users and
8 authenticate inbound email using technologies like Sender Policy Framework (SPF),
9 Domain Message Authentication Reporting and Conformance (DMARC), and
10 DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- 11 ● Scan all incoming and outgoing emails to detect threats and filter executable files
12 from reaching end users.
- 13 ● Configure firewalls to block access to known malicious IP addresses.
- 14 ● Patch operating systems, software, and firmware on devices. Consider using a
15 centralized patch management system.
- 16 ● Set anti-virus and anti-malware programs to conduct regular scans automatically.
- 17 ● Manage the use of privileged accounts based on the principle of least privilege: no
18 users should be assigned administrative access unless absolutely needed; and those
19 with a need for administrator accounts should only use them when necessary.
- 20 ● Configure access controls—including file, directory, and network share
21 permissions—with least privilege in mind. If a user only needs to read specific files,
22 the user should not have write access to those files, directories, or shares.
- 23 ● Disable macro scripts from office files transmitted via email. Consider using Office
24 Viewer software to open Microsoft Office files transmitted via email instead of full
25 office suite applications.
- 26 ● Implement Software Restriction Policies (SRP) or other controls to prevent programs
27 from executing from common ransomware locations, such as temporary folders
supporting popular Internet browsers or compression/decompression programs,
including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.¹

44. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)....
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it....
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up

¹ *Id.* at 3-4.

1 for CISA product notifications, which will alert you when a new Alert, Analysis
2 Report, Bulletin, Current Activity, or Tip has been published.

- 3 ● **Use and maintain preventative software programs.** Install antivirus software,
4 firewalls, and email filters—and keep them updated—to reduce malicious network
5 traffic....¹

6 45. To prevent and detect cyber-attacks or ransomware attacks Defendant could and
7 should have implemented, as recommended by the Microsoft Threat Protection Intelligence
8 Team, the following measures:

9 **Secure internet-facing assets**

- 10 - Apply latest security updates
11 - Use threat and vulnerability management
12 - Perform regular audit; remove privileged credentials;

13 **Thoroughly investigate and remediate alerts**

- 14 - Prioritize and treat commodity malware infections as potential full compromise;

15 **Include IT Pros in security discussions**

- 16 - Ensure collaboration among [security operations], [security admins], and
17 [information technology] admins to configure servers and other endpoints
18 securely;

19 **Build credential hygiene**

- 20 - Use [multifactor authentication] or [network level authentication] and use strong,
21 randomized, just-in-time local admin passwords;

22 **Apply principle of least-privilege**

- 23 - Monitor for adversarial activities
24 - Hunt for brute force attempts
25 - Monitor for cleanup of Event Logs
26 - Analyze logon events;

27 ¹ See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), available at: <https://us-cert.cisa.gov/ncas/tips/ST19-001> (last visited Oct. 17, 2022).

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].¹

46. Given that Defendant was storing the sensitive PII of its current and former employees, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

47. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of approximately 9,000 employees, including that of Plaintiff and Class Members.

D. Defendant Acquires, Collects, and Stores its Employees’ PII

48. As a condition of employment with Defendant, Plaintiff and Class Members were required to give their sensitive and confidential PII to Defendant.

49. Defendant retains and stores this information and derives a substantial economic benefit from the PII that it collects. But for the collection of Plaintiff’s and Class Members’ PII, Defendant would be unable to perform its products or services.

50. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were

¹ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited Nov. 11, 2021).



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

1 responsible for protecting the PII from disclosure.

2 51. Plaintiff and Class Members have taken reasonable steps to maintain the
3 confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained
4 securely, to use this information for business purposes only, and to make only authorized
5 disclosures of this information.
6

7 52. Defendant could have prevented this Data Breach by properly securing and
8 encrypting the files and file servers containing the PII of Plaintiff and Class Members.
9

10 **E. Defendant Knew or Should Have Known of the Risk Since Employers in**
11 **Possession of PII are Particularly Susceptible**
12 **to Cyber Attacks.**

13 53. Data thieves regularly target companies like Defendant's due to the highly
14 sensitive information that they custody. Defendant knew and understood that unprotected PII
15 is valuable and highly sought after by criminal parties who seek to illegally monetize that PII
16 through unauthorized access.

17 54. Defendant's data security obligations were particularly important given the
18 substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store
19 PII and other sensitive information, like Defendant, preceding the date of the breach.
20

21 55. In light of recent high profile data breaches at other industry leading companies,
22 including, Microsoft (250 million records, December 2019), Wattpad (268 million records,
23 June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records,
24 January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3
25 billion records, May 2020), Defendant knew or should have known that the PII that they
26 collected and maintained would be targeted by cybercriminals.
27

P
PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

1 56. Additionally, as companies became more dependent on computer systems to run
2 their business,¹ e.g., working remotely as a result of the Covid-19 pandemic, and the Internet
3 of Things (“IoT”), the danger posed by cybercriminals is magnified, thereby highlighting the
4 need for adequate administrative, physical, and technical safeguards.²
5

6 57. As a custodian of PII, Defendant knew, or should have known, the importance of
7 safeguarding the PII entrusted to it by Plaintiff and Class members, and of the foreseeable
8 consequences if its data security systems were breached, including the significant costs imposed
9 on Plaintiff and Class Members as a result of a breach.
10

11 58. In 2021, a record 1,862 data breaches occurred, resulting in approximately
12 293,927,708 sensitive records being exposed, a 68% increase from 2020.³

13 59. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive
14 records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive
15 records (9,700,238) in 2020.⁴
16

17 60. Despite the prevalence of public announcements of data breach and data security
18 compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class
19 Members from being compromised.
20
21
22

23 _____
24 ¹ <https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html>

25 ² <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022>

26 ³ See 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at
27 <https://notified.idtheftcenter.org/s/>), at 6.

⁴ *Id.*





PEREZ LAW GROUP, PLLC
7508 North 69th Avenue
Glendale, Arizona 85301

1 61. Indeed, cyber-attacks, such as the one experienced by Defendant, have become
2 so notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service have
3 issued a warning to potential targets so they are aware of, and prepared for, a potential attack.
4 As one report explained, smaller entities that store PII are “attractive to ransomware
5 criminals...because they often have lesser IT defenses and a high incentive to regain access to
6 their data quickly.”¹

8 62. At all relevant times, Defendant knew, or reasonably should have known, of the
9 importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable
10 consequences that would occur if Defendant's data security system was breached, including,
11 specifically, the significant costs that would be imposed on Plaintiff and Class Members as a
12 result of a breach.

14 63. Defendant was, or should have been, fully aware of the unique type and the
15 significant volume of data on Defendant's server(s), amounting to potentially thousands of
16 individuals’ detailed, PII, and, thus, the significant number of individuals who would be harmed
17 by the exposure of the unencrypted data.

19 64. In the Notice Letter, Defendant makes an offer of 12 months of identity
20 monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as
21 it fails to provide for the fact victims of data breaches and other unauthorized disclosures
22 commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to
23

24
25 _____
26 ¹https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed Oct. 17, 2022).
27

1 provide sufficient compensation for the unauthorized release and disclosure of Plaintiff and
2 Class Members’ PII. Moreover, once this service expires, Plaintiff and Class Members will be
3 forced to pay out of pocket for necessary identity monitoring services.

4 65. Defendant’s offering of credit and identity monitoring establishes that Plaintiff
5 and Class Members’ sensitive PII *was* in fact affected, accessed, compromised, and exfiltrated
6 from Defendant's computer systems.

7 66. The injuries to Plaintiff and Class Members were directly and proximately caused
8 by Defendant's failure to implement or maintain adequate data security measures for the PII of
9 Plaintiff and Class Members.

10 67. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and
11 Class Members are long lasting and severe. Once PII is stolen—particularly Social Security
12 numbers—fraudulent use of that information and damage to victims may continue for years.

13 68. As a retail employer in possession of its employees’ and former employees’ PII,
14 Defendant knew, or should have known, the importance of safeguarding the PII entrusted to
15 them by Plaintiff and Class Members and of the foreseeable consequences if its data security
16 systems were breached. This includes the significant costs imposed on Plaintiff and Class
17 Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity
18 measures to prevent the Data Breach.

19 **F. Value of Personally Identifying Information.**

20 69. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud
21 committed or attempted using the identifying information of another person without
22
23
24
25
26
27

P
PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

1 authority.”¹ The FTC describes “identifying information” as “any name or number that may be
 2 used, alone or in conjunction with any other information, to identify a specific person,”
 3 including, among other things, “[n]ame, Social Security number, date of birth, official State or
 4 government issued driver’s license or identification number, alien registration number,
 5 government passport number, employer or taxpayer identification number.”²
 6

7 70. The PII of individuals remains of high value to criminals, as evidenced by the
 8 prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen
 9 identity credentials.³ For example, Personal Information can be sold at a price ranging from \$40
 10 to \$200.⁴ Criminals can also purchase access to entire company data breaches from \$900 to
 11 \$4,500.⁵
 12

13 71. For example, Social Security numbers are among the worst kind of PII to have
 14 stolen because they may be put to a variety of fraudulent uses and are difficult for an individual
 15 to change. The Social Security Administration stresses that the loss of an individual’s Social
 16 Security number, as experienced by Plaintiff and some Class Members, can lead to identity
 17 theft and extensive financial fraud:
 18
 19
 20

21 ¹ 17 C.F.R. § 248.201 (2013).

22 ² *Id.*

23 ³ *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 Oct. 17, 2022).

24 ⁴ *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 Oct. 17, 2022).

25 ⁵ *In the Dark*, VPNOverview, 2019, available at:
 26 <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Oct. 217,
 27 2022).

1 A dishonest person who has your Social Security number can use it to get other personal
2 information about you. Identity thieves can use your number and your good credit to
3 apply for more credit in your name. Then, they use the credit cards and don't pay the
4 bills, it damages your credit. You may not find out that someone is using your number
5 until you're turned down for credit, or you begin to get calls from unknown creditors
6 demanding payment for items you never bought. Someone illegally using your Social
7 Security number and assuming your identity can cause a lot of problems.¹

8 72. What's more, it is no easy task to change or cancel a stolen Social Security
9 number. An individual cannot obtain a new Social Security number without significant
10 paperwork and evidence of actual misuse. In other words, preventive action to defend against
11 the possibility of misuse of a Social Security number is not permitted; an individual must show
12 evidence of actual, ongoing fraud activity to obtain a new number.

13 73. Even then, a new Social Security number may not be effective. According to Julie
14 Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link
15 the new number very quickly to the old number, so all of that old bad information is quickly
16 inherited into the new Social Security number."²

17 74. Based on the foregoing, the information compromised in the Data Breach is
18 significantly more valuable than the loss of, for example, credit card information in a retailer
19 data breach because, there, victims can cancel or close credit and debit card accounts. The
20 information compromised in this Data Breach is impossible to "close" and difficult, if not
21 impossible, to change—Social Security number and name.
22
23

24 _____
25 ¹ Social Security Administration, *Identity Theft and Your Social Security Number*, available
26 at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Oct. 17, 2022).

27 ² Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR
(Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last visited Oct. 17, 2022).



1 75. This data demands a much higher price on the black market. Martin Walter, senior
2 director at cybersecurity firm RedSeal, explained, “Compared to credit card information,
3 personally identifiable information and Social Security numbers are worth more than 10x on
4 the black market.”¹

5
6 76. Among other forms of fraud, identity thieves may obtain driver’s licenses,
7 government benefits, medical services, and housing or even give false information to police.

8 77. The fraudulent activity resulting from the Data Breach may not come to light for
9 years. There may be a time lag between when harm occurs versus when it is discovered, and
10 also between when PII is stolen and when it is used. According to the U.S. Government
11 Accountability Office (“GAO”), which conducted a study regarding data breaches:
12

13 [L]aw enforcement officials told us that in some cases, stolen data may be held for up to
14 a year or more before being used to commit identity theft. Further, once stolen data have
15 been sold or posted on the Web, fraudulent use of that information may continue for
16 years. As a result, studies that attempt to measure the harm resulting from data breaches
cannot necessarily rule out all future harm.²

17 78. Plaintiff and Class Members now face years of constant surveillance of their
18 financial and personal records, monitoring, and loss of rights. The Class is incurring and will
19 continue to incur such damages in addition to any fraudulent use of their PII.

20 **G. Defendant Fails to Comply with FTC Guidelines.**

21
22
23

24 ¹ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card*
25 *Numbers*, IT World, (Feb. 6, 2015), available at:
26 [https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-](https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html)
27 [10x-price-of-stolen-credit-card-numbers.html](https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html) (last visited Oct. 17, 2022).

² *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at:
<https://www.gao.gov/assets/gao-07-737.pdf> (last visited Oct. 17, 2022).

1 79. The Federal Trade Commission (“FTC”) has promulgated numerous guides for
2 businesses which highlight the importance of implementing reasonable data security practices.
3 According to the FTC, the need for data security should be factored into all business decision-
4 making.

5
6 80. In 2016, the FTC updated its publication, *Protecting Personal Information: A*
7 *Guide for Business*, which established cyber-security guidelines for businesses. These
8 guidelines note that businesses should protect the personal employee information that they
9 keep; properly dispose of personal information that is no longer needed; encrypt information
10 stored on computer networks; understand their network’s vulnerabilities; and implement
11 policies to correct any security problems.¹

12
13 81. The guidelines also recommend that businesses use an intrusion detection system
14 to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating
15 someone is attempting to hack the system; watch for large amounts of data being transmitted
16 from the system; and have a response plan ready in the event of a breach.²

17
18 82. The FTC further recommends that companies not maintain PII longer than is
19 needed for authorization of a transaction; limit access to sensitive data; require complex
20 passwords to be used on networks; use industry-tested methods for security; monitor for
21 suspicious activity on the network; and verify that third-party service providers have
22 implemented reasonable security measures.

23
24
25 _____
26 ¹ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016).
27 Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Oct. 17, 2022).

² *Id.*



1 83. The FTC has brought enforcement actions against businesses for failing to
2 adequately and reasonably protect employee data, treating the failure to employ reasonable and
3 appropriate measures to protect against unauthorized access to confidential employee data as
4 an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act
5 (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures
6 businesses must take to meet their data security obligations.
7

8 84. These FTC enforcement actions include actions against retail employers, like
9 Defendant.
10

11 85. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or
12 affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or
13 practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII.
14 The FTC publications and orders described above also form part of the basis of Defendant’s
15 duty in this regard.
16

17 86. Defendant failed to properly implement basic data security practices.

18 87. Defendant’s failure to employ reasonable and appropriate measures to protect
19 against unauthorized access to employees’ PII or to comply with applicable industry standards
20 constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.
21

22 88. Upon information and belief, Defendant was at all times fully aware of its
23 obligation to protect the PII of its employees, Defendant was also aware of the significant
24 repercussions that would result from its failure to do so. Accordingly, Defendant’s conduct was
25 particularly unreasonable given the nature and amount of PII it obtained and stored and the
26 foreseeable consequences of the immense damages that would result to Plaintiff and the Class.
27



H. Defendant Fails to Comply with Industry Standards.

1
2 89. As noted above, experts studying cyber security routinely identify entities in
3 possession of PII as being particularly vulnerable to cyberattacks because of the value of the
4 PII which they collect and maintain.

5
6 90. Several best practices have been identified that, at a minimum, should be
7 implemented by retail employers in possession of PII, like Defendant, including but not limited
8 to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-
9 virus, and anti-malware software; encryption, making data unreadable without a key; multi-
10 factor authentication; backup data and limiting which employees can access sensitive data.
11 Defendant failed to follow these industry best practices, including a failure to implement multi-
12 factor authentication.

13
14 91. Other best cybersecurity practices that are standard in the retail industry include
15 installing appropriate malware detection software; monitoring and limiting the network ports;
16 protecting web browsers and email management systems; setting up network systems such as
17 firewalls, switches and routers; monitoring and protection of physical security systems;
18 protection against any possible communication system; training staff regarding critical points.
19 Defendant failed to follow these cybersecurity best practices, including failure to train staff.

20
21 92. Defendant failed to meet the minimum standards of any of the following
22 frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation
23 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,
24 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
25
26
27

P
PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

1 for Internet Security’s Critical Security Controls (CIS CSC), which are all established standards
2 in reasonable cybersecurity readiness.

3 93. These foregoing frameworks are existing and applicable industry standards in the
4 retail industry, and upon information and belief, Defendant failed to comply with at least one–
5 –or all—of these accepted standards, thereby opening the door to the threat actor and causing
6 the Data Breach.
7

8 **I. Common Injuries and Damages.**

9 94. As a result of Defendant’s ineffective and inadequate data security practices, the
10 Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals,
11 the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent,
12 and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a)
13 invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the
14 materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain
15 (price premium damages); (d) diminution of value of their PII; and (e) the continued risk to
16 their PII, which remains in the possession of Defendant, and which is subject to further
17 breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect
18 Plaintiff’s and Class Members’ PII.
19
20
21

22 **J. The Data Breach Increases Plaintiff’s and Class Member’s
23 Risk of Identity Theft.**

24 95. The unencrypted PII of Plaintiff and Class Members will end up for sale on the
25 dark web as that is the *modus operandi* of hackers.
26
27

P
PEREZ LAW GROUP, PLLC
7508 North 69th Avenue
Glendale, Arizona 85301

1 96. Unencrypted PII may also fall into the hands of companies that will use the
2 detailed PII for targeted marketing without the approval of Plaintiff and Class Members.
3 Simply, unauthorized individuals can easily access the PII of Plaintiff and Class Members.

4 97. The link between a data breach and the risk of identity theft is simple and well
5 established. Criminals acquire and steal PII to monetize the information. Criminals monetize
6 the data by selling the stolen information on the black market to other criminals who then utilize
7 the information to commit a variety of identity theft related crimes discussed below.
8

9 98. Plaintiff’s and Class Members’ PII is of great value to hackers and cyber
10 criminals, and the data stolen in the Data Breach has been used and will continue to be used in
11 a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to profit off
12 their misfortune.
13

14 **K. Loss of Time to Mitigate the Risk of Identity Theft and Fraud.**

15 99. As a result of the recognized risk of identity theft, when a Data Breach occurs,
16 and an individual is notified by a company that their PII was compromised, as in this Data
17 Breach, the reasonable person is expected to take steps and spend time to address the dangerous
18 situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of
19 identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports
20 could expose the individual to greater financial harm – yet the resource and asset of time has
21 been lost.
22
23

24 100. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class
25 Members must, as Defendant’s Notice Letter encourages them, monitor their financial accounts
26 for many years to mitigate the risk of identity theft.
27

P
PEREZ LAW GROUP, PLLC
7508 North 89th Avenue
Glendale, Arizona 85301

1 101. Plaintiff and Class Members have spent, and will spend additional time in the
2 future, on a variety of prudent actions, such as researching the Data Breach’s occurrence,
3 researching and signing up for Defendant’s offered credit monitoring and identity theft
4 insurance, and reviewing their financial accounts for fraudulent activity, which may take years
5 to detect.
6

7 102. Plaintiff’s mitigation efforts are consistent with the U.S. Government
8 Accountability Office that released a report in 2007 regarding data breaches (“GAO Report”)
9 in which it noted that victims of identity theft will face “substantial costs and time to repair the
10 damage to their good name and credit record.”¹
11

12 103. Plaintiff’s mitigation efforts are also consistent with the steps that FTC
13 recommends that data breach victims take several steps to protect their personal and financial
14 information after a data breach, including: contacting one of the credit bureaus to place a fraud
15 alert (consider an extended fraud alert that lasts for seven years if someone steals their identity),
16 reviewing their credit reports, contacting companies to remove fraudulent charges from their
17 accounts, placing a credit freeze on their credit, and correcting their credit reports.²
18

19 104. A study by Identity Theft Resource Center shows the multitude of harms caused
20 by fraudulent use of personal and financial information:³
21

22
23 ¹ See United States Government Accountability Office, GAO-07-737, Personal Information:
24 Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However,
the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

25 ² See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps> (last
visited July 7, 2022).

26 ³ Credit Card and ID Theft Statistics” by Jason Steele, 10/24/2017, at:
27 [https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-
1276.php](https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php) (last visited Sep 13, 2022).

P
PEREZ LAW GROUP, PLLC
7508 North 89th Avenue
Glendale, Arizona 85301

P
PEREZ LAW GROUP, PLLC
 7508 North 59th Avenue
 Glendale, Arizona 85301

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27



105. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”^[4]

L. Diminution of Value of PII.

106. PII is a valuable property right.¹ Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

¹ See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (last visited Sep. 13, 2022) (“GAO Report”).

1 107. Sensitive PII can sell for as much as \$363 per record according to the Infosec
2 Institute.¹

3 108. An active and robust legitimate marketplace for PII also exists. In 2019, the data
4 brokering industry was worth roughly \$200 billion.² In fact, the data marketplace is so
5 sophisticated that consumers can actually sell their non-public information directly to a data
6 broker who in turn aggregates the information and provides it to marketers or app developers.^{3,4}
7 Consumers who agree to provide their web browsing history to the Nielsen Corporation can
8 receive up to \$50.00 a year.⁵

9
10 109. As a result of the Data Breach, Plaintiff's and Class Members' PII , which has an
11 inherent market value in both legitimate and dark markets, has been damaged and diminished
12 by its compromise and unauthorized release. However, this transfer of value occurred without
13 any consideration paid to Plaintiff or Class Members for their property, resulting in an economic
14 loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby
15 causing additional loss of value.
16
17
18
19
20

21 ¹ See, e.g., John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally
22 Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech.
23 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is
24 rapidly reaching a level comparable to the value of traditional financial assets.") (citations
25 omitted).

26 ² See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27,
27 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last visited Sep. 13, 2022).

³ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

⁴ <https://datacoup.com/>

⁵ <https://digi.me/what-is-digime/>

1 110. At all relevant times, Defendant knew, or reasonably should have known, of the
2 importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable
3 consequences that would occur if Defendant’s data security system was breached, including,
4 specifically, the significant costs that would be imposed on Plaintiff and Class Members as a
5 result of a breach.
6

7 111. The fraudulent activity resulting from the Data Breach may not come to light for
8 years.
9

10 112. Plaintiff and Class Members now face years of constant surveillance of their
11 financial and personal records, monitoring, and loss of rights. The Class is incurring and will
12 continue to incur such damages in addition to any fraudulent use of their PII .

13 113. Defendant was, or should have been, fully aware of the unique type and the
14 significant volume of data on Defendant’s network, amounting to potentially thousands of
15 individuals’ detailed personal information and, thus, the significant number of individuals who
16 would be harmed by the exposure of the unencrypted data.
17

18 114. The injuries to Plaintiff and Class Members were directly and proximately caused
19 by Defendant’s failure to implement or maintain adequate data security measures for the PII of
20 Plaintiff and Class Members.
21

22 **M. Future Costs of Credit and Identity Theft Monitoring is**
23 **Reasonable and Necessary.**

24 115. Given the type of targeted attack, the sophisticated criminal activity, and the type
25 of PII involved in this case, there is a strong probability that entire batches of stolen information
26 have been placed, or will be placed, on the black market/dark web for sale and purchase by
27

P
PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

1 criminals intending to utilize the PII for identity theft crimes –e.g., opening bank accounts in
2 the victims’ names to make purchases or to launder money; file false tax returns; take out loans
3 or lines of credit; or file false unemployment claims.

4 116. Such fraud may go undetected until debt collection calls commence months, or
5 even years, later. An individual may not know that his or her PII was used to file for
6 unemployment benefits until law enforcement notifies the individual’s employer of the
7 suspected fraud. Fraudulent tax returns are typically discovered only when an individual’s
8 authentic tax return is rejected.
9

10 117. Consequently, Plaintiff and Class Members are at an increased risk of fraud and
11 identity theft for many years into the future.
12

13 118. The retail cost of credit monitoring and identity theft monitoring can cost around
14 \$200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class
15 Members from the risk of identity theft that arose from Defendant’s Data Breach. This is a
16 future cost for a minimum of five years that Plaintiff and Class Members would not need to
17 bear but for Defendant’s failure to safeguard their PII .
18

19 **N. Loss of Benefit of the Bargain.**

20 119. Furthermore, Defendant’s poor data security deprived Plaintiff and Class
21 Members of the benefit of their bargain. When agreeing to provide their labor and PII to
22 Defendant, Plaintiff and other reasonable employees understood and expected that they were,
23 in part, providing their labor and PII to Defendant ,and in return, Defendant would, among other
24 things, adequately safeguard their PII. However, Defendant did not provide the expected data
25
26
27

P
PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

1 security. Accordingly, Plaintiff and Class Members received employment of a lesser value than
2 what they reasonably expected to receive under the bargains they struck with Defendant.

3 **O. Plaintiff Barrios’ Experience.**

4 120. Prior to the Data Breach Plaintiff Barrios was employed at Defendant for
5 approximately one year from 1998 to 1999. In the course of enrolling in employment with
6 Defendant and as a condition of employment, she was required to supply Defendant with her
7 PII, including but not limited to her name, date of birth, and Social Security number.
8

9 121. Plaintiff Barrios is very careful about sharing her sensitive PII. Plaintiff stores
10 any documents containing her PII in a safe and secure location. She has never knowingly
11 transmitted unencrypted sensitive PII over the internet or any other unsecured source.
12

13 122. At the time of the Data Breach—May 31, 2022— Defendant retained Plaintiff
14 Barrios’ PII in its system, despite the fact that Plaintiff stopped working at Defendant more
15 than two decades prior.
16

17 123. Plaintiff Barrios received the Notice Letter, by U.S. mail, directly from
18 Defendant, dated January 12, 2023. According to the Notice Letter, Plaintiff Barrios’ PII
19 was improperly accessed and obtained by unauthorized third parties, including her name,
20 date of birth, and Social Security number.
21

22 124. Upon receiving the Notice Letter from Defendant, Plaintiff Barrios also spent
23 time dealing with the consequences of the Data Breach, including time spent researching the
24 Data Breach, reviewing her financial accounts for fraudulent activity, and enrolling in credit
25 monitoring and identity theft insurance. This time has been lost forever and cannot be
26 recaptured.
27

P

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

1 125. Subsequent to the Data Breach, Plaintiff Barrios has suffered numerous,
2 substantial injuries including, but not limited to, (i) invasion of privacy; (ii) the diminution
3 of the value of her PII (iii) loss of benefit of the bargain; and (iv) the continued and certainly
4 increased risk to her PII, which: (a) remains unencrypted and available for unauthorized
5 third parties to access and abuse; and (b) remain backed up in Defendant’s possession and
6 is subject to further unauthorized disclosures so long as Defendant fails to undertake
7 appropriate and adequate measures to protect her PII.
8

9 126. Plaintiff Barrios additionally suffered actual injury and damages as a result of the
10 Data Breach. Implied in her employment contract with Defendant was the requirement that it
11 adequately safeguard her PII. Plaintiff Barrios would not have worked for Defendant had
12 Defendant disclosed that it lacked data security practices adequate to safeguard PII.
13

14 127. Plaintiff Barrios further suffered actual injury in the form of damages and
15 diminution in the value of her PII—a form of intangible property that she entrusted to Defendant
16 for the purpose of employment, which was compromised by the Data Breach.
17

18 128. Plaintiff Barrios also suffered lost time, annoyance, interference, and
19 inconvenience as a result of the Data Breach and has anxiety and increased concerns for the
20 loss of her privacy, especially her Social Security number.
21

22 129. Plaintiff Barrios has suffered imminent and impending injury arising from the
23 substantially increased risk of fraud, identity theft, and misuse resulting from her stolen PII,
24 especially her Social Security number, being placed in the hands of unauthorized third parties
25 and possibly criminals.
26
27

P
PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

1 130. Plaintiff Barrios has a continuing interest in ensuring that her PII, which, upon
2 information and belief, remains backed up in Defendant’s possession, is protected and
3 safeguarded from future breaches.

4 **V. CLASS ACTION ALLEGATIONS**

5
6 131. Plaintiff brings this action on her own behalf and on behalf of all others similarly
7 situated under Rule 23(a), (b)(3), and (c)(4) of the Federal Rules of Civil Procedure.

8 132. The Class that Plaintiff seeks to represent is defined as follows:

9 All individuals residing in the United States whose PII was accessed and/or acquired by an
10 unauthorized party as a result of the data breach reported by Defendant on or about
11 January 12, 2023 (the “Class”).

12 133. Excluded from the Class are the following individuals and/or entities: Defendant
13 and Defendant’s parents, subsidiaries, affiliates, officers and directors, and any entity in which
14 Defendant have a controlling interest; all individuals who make a timely election to be excluded
15 from this proceeding using the correct protocol for opting out; and all judges assigned to hear
16 any aspect of this litigation, as well as their immediate family members.

17
18 134. Plaintiff reserves the right to amend the definitions of the Class or add a Class
19 or Subclass if further information and discovery indicate that the definitions of the Class
20 should be narrowed, expanded, or otherwise modified.

21
22 135. Numerosity. The members of the Class are so numerous that joinder of all
23 members is impracticable, if not completely impossible. At least 8,000 individuals were notified
24 by Defendant of the Data Breach, according to the breach report submitted to Maine Attorney
25
26
27

P
PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

1 General's Office.¹ The Class is apparently identifiable within Defendant's records, and
2 Defendant has already identified these individuals (as evidenced by sending them breach
3 notification letters).

4 136. Common questions of law and fact exist as to all members of the Class and
5 predominate over any questions affecting solely individual members of the Class. Among the
6 questions of law and fact common to the Class that predominate over questions which may
7 affect individual Class members, including the following:
8

- 9 a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff
10 and Class Members;
- 11 b. Whether Defendant had respective duties not to disclose the PII of Plaintiff and
12 Class Members to unauthorized third parties;
- 13 c. Whether Defendant had respective duties not to use the PII of Plaintiff and Class
14 Members for non-business purposes;
- 15 d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class
16 Members;
- 17 e. Whether and when Defendant actually learned of the Data Breach;
- 18 f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and
19 Class Members that their PII had been compromised;
- 20 g. Whether Defendant violated the law by failing to promptly notify Plaintiff and
21 Class Members that their PII had been compromised;
- 22
- 23
- 24
- 25

26 _____
27 ¹ <https://apps.web.maine.gov/online/aeviewer/ME/40/176917d7-3364-41bd-9b16-80e11da3f497.shtml>

- 1 h. Whether Defendant failed to implement and maintain reasonable security
- 2 procedures and practices appropriate to the nature and scope of the information
- 3 compromised in the Data Breach;
- 4 i. Whether Defendant adequately addressed and fixed the vulnerabilities which
- 5 permitted the Data Breach to occur;
- 6 j. Whether Plaintiff and Class Members are entitled to actual damages, statutory
- 7 damages, and/or nominal damages as a result of Defendant’s wrongful conduct;
- 8 and,
- 9 k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress
- 10 the imminent and currently ongoing harm faced as a result of the Data Breach.

11 137. Typicality. Plaintiff’s claims are typical of those of the other members of the

12 Class because Plaintiff, like every other Class Member, was exposed to virtually identical

13 conduct and now suffers from the same violations of the law as each other member of the Class.

14 138. Policies Generally Applicable to the Class. This class action is also appropriate

15 for certification because Defendant acted or refused to act on grounds generally applicable to

16 the Class, thereby requiring the Court’s imposition of uniform relief to ensure compatible

17 standards of conduct toward the Class Members and making final injunctive relief appropriate

18 with respect to the Class as a whole. Defendant’s policies challenged herein apply to and affect

19 Class Members uniformly and Plaintiff’s challenge of these policies hinges on Defendant’s

20 conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

21 139. Adequacy. Plaintiff will fairly and adequately represent and protect the interests

22 of the Class Members in that he has no disabling conflicts of interest that would be antagonistic



1 to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to
2 the Class Members and the infringement of the rights and the damages she has suffered are
3 typical of other Class Members. Plaintiff has retained counsel experienced in complex class
4 action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

5
6 140. Superiority and Manageability. The class litigation is an appropriate method for
7 fair and efficient adjudication of the claims involved. Class action treatment is superior to all
8 other available methods for the fair and efficient adjudication of the controversy alleged herein;
9 it will permit a large number of Class Members to prosecute their common claims in a single
10 forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort,
11 and expense that hundreds of individual actions would require. Class action treatment will
12 permit the adjudication of relatively modest claims by certain Class Members, who could not
13 individually afford to litigate a complex claim against large corporations, like Defendant.
14 Further, even for those Class Members who could afford to litigate such a claim, it would still
15 be economically impractical and impose a burden on the courts.
16
17

18 141. The nature of this action and the nature of laws available to Plaintiff and Class
19 Members make the use of the class action device a particularly efficient and appropriate
20 procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because
21 Defendant would necessarily gain an unconscionable advantage since they would be able to
22 exploit and overwhelm the limited resources of each individual Class Member with superior
23 financial and legal resources; the costs of individual suits could unreasonably consume the
24 amounts that would be recovered; proof of a common course of conduct to which Plaintiff was
25 exposed is representative of that experienced by the Class and will establish the right of each
26
27

P
PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

1 Class Member to recover on the cause of action alleged; and individual actions would create a
2 risk of inconsistent results and would be unnecessary and duplicative of this litigation.

3 142. The litigation of the claims brought herein is manageable. Defendant's uniform
4 conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class
5 Members demonstrates that there would be no significant manageability problems with
6 prosecuting this lawsuit as a class action.

7
8 143. Adequate notice can be given to Class Members directly using information
9 maintained in Defendant's records.

10
11 144. Unless a Class-wide injunction is issued, Defendant may continue in its failure to
12 properly secure the PII of Class Members, Defendant may continue to refuse to provide proper
13 notification to Class Members regarding the Data Breach, and Defendant may continue to act
14 unlawfully as set forth in this Complaint.

15
16 145. Further, Defendant has acted on grounds that apply generally to the Class as a
17 whole, so that class certification, injunctive relief, and corresponding declaratory relief are
18 appropriate on a class- wide basis.

19
20 146. Likewise, particular issues under Rule 23(c)(2) are appropriate for certification
21 because such claims present only particular, common issues, the resolution of which would
22 advance the disposition of this matter and the parties' interests therein. Such particular issues
23 include, but are not limited to:

- 24 a. Whether Defendant failed to timely notify the Plaintiff and the class of the Data
25 Breach;
26
27

- b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;
- c. Whether Defendant’s security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;
- d. Whether Defendant’s failure to institute adequate protective security measures amounted to negligence;
- e. Whether Defendant failed to take commercially reasonable steps to safeguard its employees’ PII; and,
- f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

VI. CAUSES OF ACTION

**COUNT I
NEGLIGENCE**

(On Behalf of Plaintiff and All Class Members)

147. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 146 above as if fully set forth herein.

148. Defendant required Plaintiff and Class Members to submit non-public PII as a condition of employment or as a condition of receiving employee benefits.

149. Plaintiff and the Class Members entrusted their PII to Defendant with the understanding that Defendant would safeguard their information and delete it once it was no longer required to retain it after the end of the employment relationship.



PEREZ LAW GROUP, PLLC
7508 North 69th Avenue
Glendale, Arizona 85301

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

1 150. Defendant had a duty to employ reasonable security measures and otherwise
2 protect the PII of Plaintiff and Class Members.

3 151. Defendant had full knowledge of the sensitivity of the PII and the types of harm
4 that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.
5

6 152. By assuming the responsibility to collect and store this data, and in fact doing so,
7 and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable
8 means to secure and safeguard their computer property—and Class Members’ PII held within
9 it—to prevent disclosure of the information, and to safeguard the information from theft.
10 Defendant’s duty included a responsibility to implement processes by which they could detect
11 a breach of its security systems in a reasonably expeditious period of time and to give prompt
12 notice to those affected in the case of a data breach.
13

14 153. Defendant had a duty to employ reasonable security measures under Section 5 of
15 the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or
16 affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of
17 failing to use reasonable measures to protect confidential data.
18

19 154. Defendant’s duty to use reasonable care in protecting confidential data arose not
20 only as a result of the statutes and regulations described above, but also because Defendant is
21 bound by industry standards to protect confidential PII.
22

23 155. Defendant breached its duties, and thus was negligent, by failing to use
24 reasonable measures to protect Class Members’ PII. The specific negligent acts and omissions
25 committed by Defendant include, but are not limited to, the following:
26
27

P
PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

- 1 a. Failing to adopt, implement, and maintain adequate security measures to
- 2 safeguard Class Members’ PII;
- 3 b. Failing to adequately monitor the security of their networks and systems;
- 4 c. Failing to periodically ensure that their email system had plans in place to
- 5 maintain reasonable data security safeguards;
- 6 d. Allowing unauthorized access to Class Members’ PII; and
- 7 e. Failing to detect in a timely manner that Class Members’ PII had been
- 8 compromised.
- 9
- 10

11 156. It was foreseeable that Defendant’s failure to use reasonable measures to protect
 12 Class Members’ PII would result in injury to Class Members. Further, the breach of security
 13 was reasonably foreseeable given the known high frequency of cyberattacks and data breaches
 14 in the industry.

15 157. It was therefore foreseeable that the failure to adequately safeguard Class
 16 Members’ PII would result in one or more types of injuries to Class Members.
 17

18 158. There is a temporal and close causal connection between Defendant’s failure to
 19 implement security measures to protect the PII and the harm suffered, or risk of imminent harm
 20 suffered by Plaintiff and the Class.
 21

22 159. As a result of Defendant’s negligence, Plaintiff and the Class Members have
 23 suffered and will continue to suffer damages and injury including, but not limited to: (i) lost or
 24 diminished value of PII; (ii) lost opportunity costs associated with attempting to mitigate the
 25 actual consequences of the Data Breach, including but not limited to lost time, (iii) invasion of
 26 privacy; and (iv) the continued and certainly increased risk to their PII, which: (a) remains
 27



1 unencrypted and available for unauthorized third parties to access and abuse; and (b) remains
2 backed up in Defendant’s possession and is subject to further unauthorized disclosures so long
3 as Defendant fails to undertake appropriate and adequate measures to protect the PII.

4 160. Plaintiff and Class Members are entitled to compensatory and consequential
5 damages suffered as a result of the Data Breach.

6 161. Plaintiff and Class Members are also entitled to injunctive relief requiring
7 Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii)
8 submit to future annual audits of those systems and monitoring procedures; and (iii) continue
9 to provide adequate credit monitoring to all Class Members.
10
11

12 **COUNT II**
13 **NEGLIGENCE *PER SE***
14 **(On Behalf of Plaintiff and All Class Members)**

15 162. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 161 above
16 as if fully set forth herein.

17 163. Pursuant to Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45),
18 Defendant had a duty to provide fair and adequate computer systems and data security practices
19 to safeguard Plaintiff’s and Class Members’ PII.

20 164. Defendant breached its duties to Plaintiff and Class Members under the Federal
21 Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems
22 and data security practices to safeguard Plaintiff’s and Class Members’ PII.

23 165. Plaintiff and Class Members are within the class of persons the FTC Act was
24 intended to protect and the harm resulting from the Data Breach is the type of injury against
25 which the FTC Act was intended to guard.
26
27

P
PEREZ LAW GROUP, PLLC
7508 North 69th Avenue
Glendale, Arizona 85301

1 166. Defendant’s failure to comply with applicable laws and regulations constitutes
2 negligence *per se*.

3 167. But for Defendant’s wrongful and negligent breach of its duties owed to Plaintiff
4 and Class Members, Plaintiff and Class Members would not have been injured.

5 168. The injury and harm suffered by Plaintiff and Class Members was the reasonably
6 foreseeable result of Defendant’s breach of its duties. Defendant knew or should have known
7 that it was failing to meet its duties, and that Defendant’s breach would cause Plaintiff and
8 Class Members to experience the foreseeable harms associated with the exposure of their PII.
9

10 169. As a direct and proximate result of Defendant’s negligent conduct, Plaintiff and
11 Class Members have suffered injury and are entitled to compensatory, consequential, and
12 punitive damages in an amount to be proven at trial.
13

14 **COUNT III**
15 **BREACH OF IMPLIED CONTRACT**
16 **(On Behalf of Plaintiff and All Class Members)**

17 170. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 169 above
18 as if fully set forth herein.

19 171. Plaintiff and Class Members were required to provide their PII to Defendant as a
20 condition of their employment with Defendant.
21

22 172. Plaintiff and Class Members provided their labor to Defendant in exchange for
23 (among other things) Defendant’s promise to protect their PII from unauthorized disclosure and
24 to delete it once it was no longer necessary to maintain the PII for employment purposes.
25

26 173. On information and belief, at all relevant times Defendant promulgated, adopted,
27 and implemented written privacy policies whereby it expressly promised Plaintiff and Class

P
PEREZ LAW GROUP, PLLC
7508 North 89th Avenue
Glendale, Arizona 85301

1 Members that it would only disclose PII under certain circumstances, none of which relate to
2 the Data Breach.

3 174. On information and belief, Defendant further promised to comply with industry
4 standards and to make sure that Plaintiff’s and Class Members’ PII would remain protected.
5

6 175. Implicit in the agreement between Plaintiff and Class Members and the Defendant
7 to provide PII, was the latter’s obligation to: (a) use such PII for business purposes only, (b)
8 take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d)
9 provide Plaintiff and Class Members with prompt and sufficient notice of any and all
10 unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of
11 Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the PII only
12 under conditions that kept such information secure and confidential.
13

14 176. When Plaintiff and Class Members provided their PII to Defendant as a condition
15 of their employment or employee beneficiary status, they entered into implied contracts with
16 Defendant pursuant to which Defendant agreed to reasonably protect such information.
17

18 177. Defendant required Class Members to provide their PII as part of Defendant’s
19 regular business practices. Plaintiff and Class Members accepted Defendant’s offers and
20 provided their PII to Defendant.
21

22 178. In entering into such implied contracts, Plaintiff and Class Members reasonably
23 believed and expected that Defendant’s data security practices complied with relevant laws and
24 regulations and were consistent with industry standards.
25

26 179. Plaintiff and Class Members would not have entrusted their PII to Defendant in
27 the absence of the implied contract between them and Defendant to keep their information

P
PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

1 reasonably secure. Plaintiff and Class Members would not have entrusted their PII to Defendant
2 in the absence of its implied promise to monitor its computer systems and networks to ensure
3 that it adopted reasonable data security measures.

4 180. Plaintiff and Class Members fully and adequately performed their obligations
5 under the implied contracts with Defendant.
6

7 181. Defendant breached its implied contracts with Class Members by failing to
8 safeguard and protect their PII.

9 182. As a direct and proximate result of Defendant’s breaches of the implied contracts,
10 Class Members sustained damages as alleged herein.
11

12 183. Plaintiff and Class Members are entitled to compensatory and consequential
13 damages suffered as a result of the Data Breach.

14 184. Plaintiff and Class Members are also entitled to nominal damages for the breach
15 of implied contract.
16

17 185. Plaintiff and Class Members are also entitled to injunctive relief requiring
18 Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii)
19 submit to future annual audits of those systems and monitoring procedures; and (iii)
20 immediately provide adequate credit monitoring to all Class Members.
21

22 **COUNT IV**
23 **UNJUST ENRICHMENT**
24 **(On Behalf of Plaintiff and All Class Members)**

25 186. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 185 above
26 as if fully set forth herein.
27

P
PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

1 187. This Count is pleaded in the alternative to the breach of implied contract (Count
2 III).

3 188. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the
4 form of their labor and by providing their valuable PII to Defendant.
5

6 189. Plaintiff and Class Members provided Defendant their labor and PII on the
7 understanding that Defendant would pay for the administrative costs of reasonable data privacy
8 and security practices and procedures. In exchange, Plaintiff and Class members should have
9 received adequate protection and data security for such PII held by Defendant.
10

11 190. Defendant benefited from receiving Plaintiff's and Class Members' labor and
12 from receiving their PII through its ability to retain and use that information for its own benefit.
13 Defendant understood and accepted this benefit.

14 191. Defendant knew Plaintiff and Class members conferred a benefit which
15 Defendant accepted. Defendant profited from Plaintiff's and Class Members' labor and used
16 their PII for business purposes.
17

18 192. Because all PII provided by Plaintiff and Class Members was similarly at risk
19 from a foreseeable and targeted data breach, Defendant's obligation to safeguard the PII it
20 collected from its employees was inherent to the employment relationship.
21

22 193. Defendant also understood and appreciated that Plaintiff's and Class Members'
23 PII was private and confidential, and its value depended upon Defendant maintaining the
24 privacy and confidentiality of that information.
25

26 194. Defendant failed to provide reasonable security, safeguards, and protections to
27 the PII of Plaintiff and Class Members.

P
PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

1 195. Defendant enriched itself by saving the costs it reasonably should have expended
2 on data security measures to secure Plaintiff’s and Class Members’ PII.

3 196. Instead of providing a reasonable level of security that would have prevented the
4 Data Breach, Defendant instead made calculated decisions to increase its profits at the expense
5 of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and
6 Class Members, on the other hand, suffered as a direct and proximate result of Defendant’s
7 failure to provide the requisite security.
8

9 197. Under the principles of equity and good conscience, Defendant should not be
10 permitted to retain money belonging to Plaintiff and Class Members, because Defendant failed
11 to implement appropriate data management and security measures mandated by industry
12 standards.
13

14 198. Defendant’s enrichment at the expense of Plaintiff and Class Members is and was
15 unjust.
16

17 199. Defendant acquired the monetary benefit and PII through inequitable means in
18 that they failed to disclose the inadequate security practices previously alleged.

19 200. If Plaintiff and Class Members knew that Defendant had not secured their PII,
20 they would not have agreed to provide their PII to Defendant.
21

22 201. Plaintiff and Class Members have no adequate remedy at law.

23 202. As a direct and proximate result of Defendant’s conduct, Plaintiff and Class
24 Members have suffered and will suffer injury as described herein.
25
26
27

P
PEREZ LAW GROUP, PLLC
7508 North 69th Avenue
Glendale, Arizona 85301

1 203. Plaintiff and the Class Members are entitled to restitution and disgorgement of all
 2 profits, benefits, and other compensation obtained by Defendant, plus attorneys’ fees, costs,
 3 and interest thereon.

4 **PRAYER FOR RELIEF**

5 WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment
 6 against Defendant and that the Court grants the following:
 7

- 8 A. For an order certifying the Class, as defined herein, and appointing Plaintiff and
- 9 her Counsel to represent the Class;
- 10 B. For equitable relief enjoining Defendant from engaging in the wrongful conduct
- 11 complained of herein pertaining to the misuse and/or disclosure of the PII of
- 12 Plaintiff and Class Members, and from refusing to issue prompt, complete, any
- 13 accurate disclosures to Plaintiff and Class Members;
- 14 C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive
- 15 and other equitable relief as is necessary to protect the interests of Plaintiff and
- 16 Class Members, including but not limited to an order:
- 17 i. prohibiting Defendant from engaging in the wrongful and unlawful acts
- 18 described herein;
- 19 ii. requiring Defendant to protect, including through encryption, all data
- 20 collected through the course of its business in accordance with all
- 21 applicable regulations, industry standards, and federal, state, or local laws.
- 22 iii. requiring Defendant to delete, destroy, and purge the personal identifying
- 23 information of Plaintiff and Class Members unless Defendant can provide
- 24 information of Plaintiff and Class Members unless Defendant can provide
- 25 information of Plaintiff and Class Members unless Defendant can provide
- 26 information of Plaintiff and Class Members unless Defendant can provide
- 27 information of Plaintiff and Class Members unless Defendant can provide



PEREZ LAW GROUP, PLLC
 7508 North 99th Avenue
 Glendale, Arizona 85301



PEREZ LAW GROUP, PLLC
7508 North 69th Avenue
Glendale, Arizona 85301

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

- iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;
- v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;
- vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant’s systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
- ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant’s network is compromised, hackers cannot gain access to other portions of Defendant’s systems;



PEREZ LAW GROUP, PLLC
7508 North 69th Avenue
Glendale, Arizona 85301

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

- x. requiring Defendant to conduct regular database scanning and securing checks;
- xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees’ respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
- xii. requiring Defendant to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xiii. requiring Defendant to implement a system of tests to assess its employees’ knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees’ compliance with Defendant’s policies, programs, and systems for protecting personal identifying information;
- xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant’s information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;



PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant’s servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant’s compliance with the terms of the Court’s final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court’s final judgment;

- D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys’ fees and costs as allowed by law;
- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff, individually and on behalf of the Class, hereby demands a trial by jury on all claims so triable.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

DATED this 24th day of April, 2023.

PEREZ LAW GROUP, PLLC

/s/ Cristina Perez Hesano
Cristina Perez Hesano, Esq.
Attorney for Plaintiff and the Putative Class

Gary M. Klinger*
**MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN PLLC**
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

**Pro Hac Vice Forthcoming*

*Attorneys for Plaintiff and
the Putative Class*



ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Green Valley Pecan Company Hit with Class Action Over May 2022 Data Breach](#)
