UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

Jeffrey Ebert, on behalf of himself and on behalf of his **minor children M.E., E.E., and S.E.**, and **Jennifer Ebert**, on behalf of herself, and collectively on behalf of all others similarly situated,

Plaintiffs,

v.

PRGX Global, Inc.,

Defendant.

Case No. 1:23-CV-04233-TWT

JURY TRIAL DEMANDED

FIRST AMENDED CLASS ACTION COMPLAINT

COMES NOW Plaintiffs Jeffrey Ebert, individually and on behalf of his minor children M.E., E.E., and S.E., and Jennifer Ebert ("Plaintiffs"), individually, and collectively on behalf of all other similarly situated individuals (the "Class" or "Class Members," as defined below), by and through their undersigned counsel, file this First Amended Class Action Complaint against PRGX Global Inc., a Georgia corporation ("PRGX" or "Defendant") and allege the following based on personal knowledge of facts, upon information and belief, and based on the investigation of counsel as to all other matters.

I. NATURE OF THE ACTION

1. Plaintiffs bring this class action lawsuit against PRGX for its ongoing failure to protect and safeguard Plaintiffs' and the Class's highly sensitive personally identifiable information ("PII"). As a result of PRGX's insufficient data security, cybercriminals easily infiltrated Defendant's inadequately protected computer systems and ***stole*** the PII of Plaintiffs and the Class in not one, but ***two data breaches*** (collectively, the "Data Breaches"). Now, Plaintiffs' and the Class's PII is in the hands of cybercriminals who will use their PII for nefarious purposes for the rest of their lives.

2. The first Data Breach PRGX failed to prevent was perpetrated in or around April 2022 (the "First Data Breach" or the "First Breach").[1]

3. According to PRGX, on April 9, 2022, PRGX noticed that certain computer servers and systems storing Plaintiffs' and the Class's PII were inaccessible.[2]

---

[1] *See* Exhibits 1–5.

[2] *Data Breach Notifications*, OFFICE OF THE MAINE ATTORNEY GENERAL, https://apps.web.maine.gov/online/aeviewer/ME/40/f674c5b1-aad3-4c7f-84ac-422031509727.shtml (last visited Oct. 9, 2023).

4. After an investigation, PRGX determined that "***an unknown actor accessed [its] systems between April 8, 2022 and April 9, 2022, and took or viewed certain files***" containing the PII of Plaintiffs and the Class.[3]

5. PRGX conceded that the types of PII accessed in the First Data Breach included highly sensitive information such as: (i) names; (ii) Social Security numbers; and (iii) financial information (account numbers and/or credit/debit card numbers in combination with security codes, access codes, passwords or PINs for the accounts).[4]

6. Although PRGX learned of the First Data Breach on April 9, 2022, PRGX did not notify victims of the First Data Breach until on or around May 5, 2023, ***over a year*** after PRGX learned of the First Data Breach.[5]

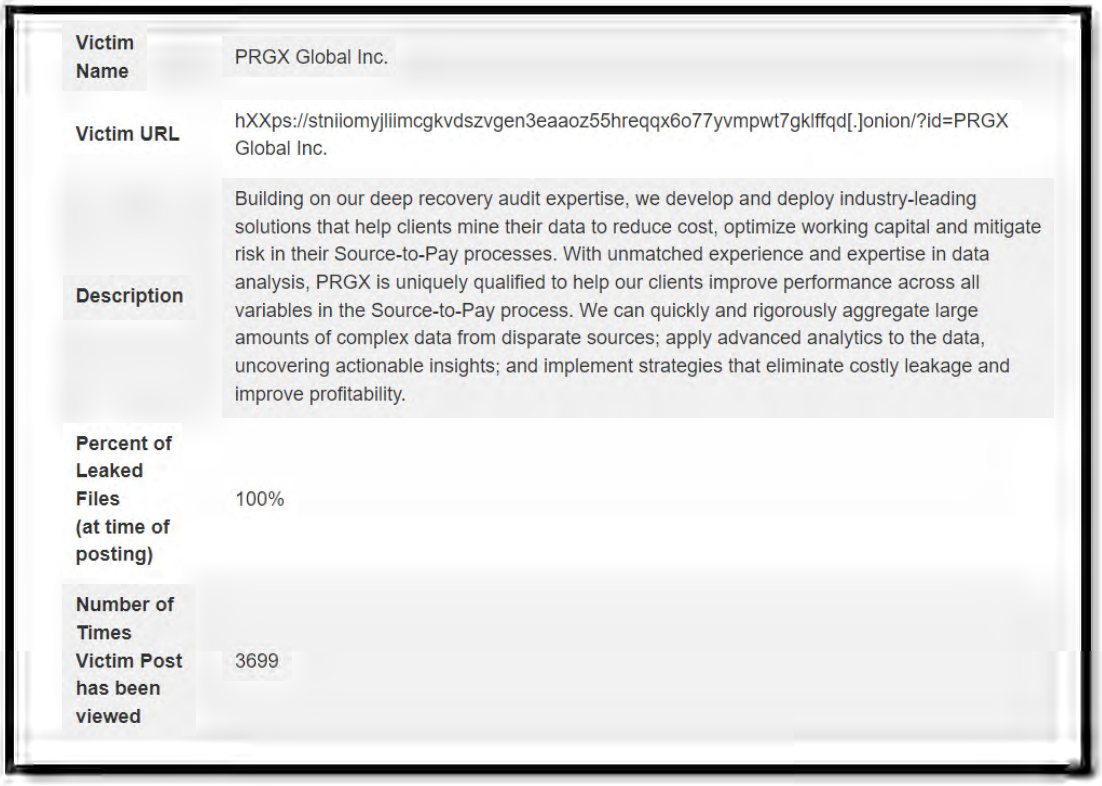
---

[3] *See* Exhibits 1–5 (emphasis added); *see also Data Breach Notifications*, OFFICE OF THE MAINE ATTORNEY GENERAL, https://apps.web.maine.gov/online/aeviewer/ME/40/f674c5b1-aad3-4c7f-84ac-422031509727.shtml (PRGX determined certain files on its systems "may have been viewed or downloaded.") (last visited Oct. 9, 2023).

[4] *See Data Breach Notifications*, OFFICE OF THE MAINE ATTORNEY GENERAL, https://apps.web.maine.gov/online/aeviewer/ME/40/f674c5b1-aad3-4c7f-84ac-422031509727.shtml (last visited Oct. 9, 2023).

[5] *See* Exhibits 1–5.

7. After the First Data Breach, several sources, like the one pictured below, reported Black Basta Group ("Black Basta"), a criminal ransomware group, was responsible for the First Breach:[6]



Victim Name	PRGX Global Inc.
Victim URL	hXXps://stniiomyjliimcgkvdszvgen3eaaoz55hreqqx6o77yvmpwt7gklffqd[.]onion/?id=PRGX Global Inc.
Description	Building on our deep recovery audit expertise, we develop and deploy industry-leading solutions that help clients mine their data to reduce cost, optimize working capital and mitigate risk in their Source-to-Pay processes. With unmatched experience and expertise in data analysis, PRGX is uniquely qualified to help our clients improve performance across all variables in the Source-to-Pay process. We can quickly and rigorously aggregate large amounts of complex data from disparate sources; apply advanced analytics to the data, uncovering actionable insights; and implement strategies that eliminate costly leakage and improve profitability.
Percent of Leaked Files (at time of posting)	100%
Number of Times Victim Post has been viewed	3699

8. "Like other enterprise-targeting ransomware operations, Black Basta will steal corporate data and documents before encrypting a company's devices. This

---

[6] *See Black Basta Ransomware Victim: PRGX Global Inc[.]*, REDPACKET SECURITY, https://www.redpacketsecurity.com/black-basta-ransomware-victim-prgx-global-inc/ (last visited Oct. 9, 2023); *Weekly Dark Web Trends/Advisory*, CYFIRMA, *available at* https://www.prianto.com/fileadmin/user_upload/PRIANTO_CEE/Cyfirma/Weekly_Dark_Web_Trends_and_Advisory_13_May_2022.pdf (last visited Oct. 9, 2023); *Profiles for ransomware group: blackbasta*, RANSWOMWARE.LIVE, https://www.ransomware.live/#/group/blackbasta (last visited Oct. 9, 2023); RANSOMLOOK, https://www.ransomlook.io/search (input "PRGX" in the search bar) (last visited Oct. 9, 2023).

stolen data is then used in double-extortion attacks, where the threat actors demand a ransom to receive a decryptor and prevent the publishing of the victim's stolen data. The data extortion part of these attacks is conducted on the 'Black Basta Blog' or 'Basta News' Tor site, which contains a list of all victims who have not paid a ransom. Black Basta will slowly leak data for each victim to try and pressure them into paying a ransom."[7]

9. Black Basta's "encryption algorithm is secure and [] there is no way to recover files for free."[8]

10. Plaintiffs and the Class were left in the dark for over a year regarding the theft of their PII and whether PRGX was able to retrieve it.

11. PRGX has offered no assurance it paid Black Basta's ransom demand to retrieve Plaintiffs' and the Class's data and prevent it from being posted on the dark web.

---

[7] Lawrence Abrams, *New Black Basta ransomware spring into action with a dozen breaches*, BLEEPINGCOMPUTER (April 27, 2022, 5:46 PM), https://www.bleepingcomputer.com/news/security/new-black-basta-ransomware-springs-into-action-with-a-dozen-breaches/ (last visited Oct. 9, 2023); *HC3 Threat Profile*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES HEALTH SECTOR CYBERSECURITY COORDINATION CENTER (Mar. 15, 2023), *available at* https://www.hhs.gov/sites/default/files/black-basta-threat-profile.pdf.

[8] Lawrence Abrams, *New Black Basta ransomware spring into action with a dozen breaches*, BLEEPINGCOMPUTER (April 27, 2022, 5:46 PM), https://www.bleepingcomputer.com/news/security/new-black-basta-ransomware-springs-into-action-with-a-dozen-breaches/ (last visited Oct. 9, 2023).

12. Even if PRGX did pay Black Basta's ransom demand that does not mean Black Basta will not post and/or sell Plaintiffs' and the Class's PII on the dark web in the future, doubling its profits. After all, Black Basta is known to be a "financially motivated" ransomware group.[9]

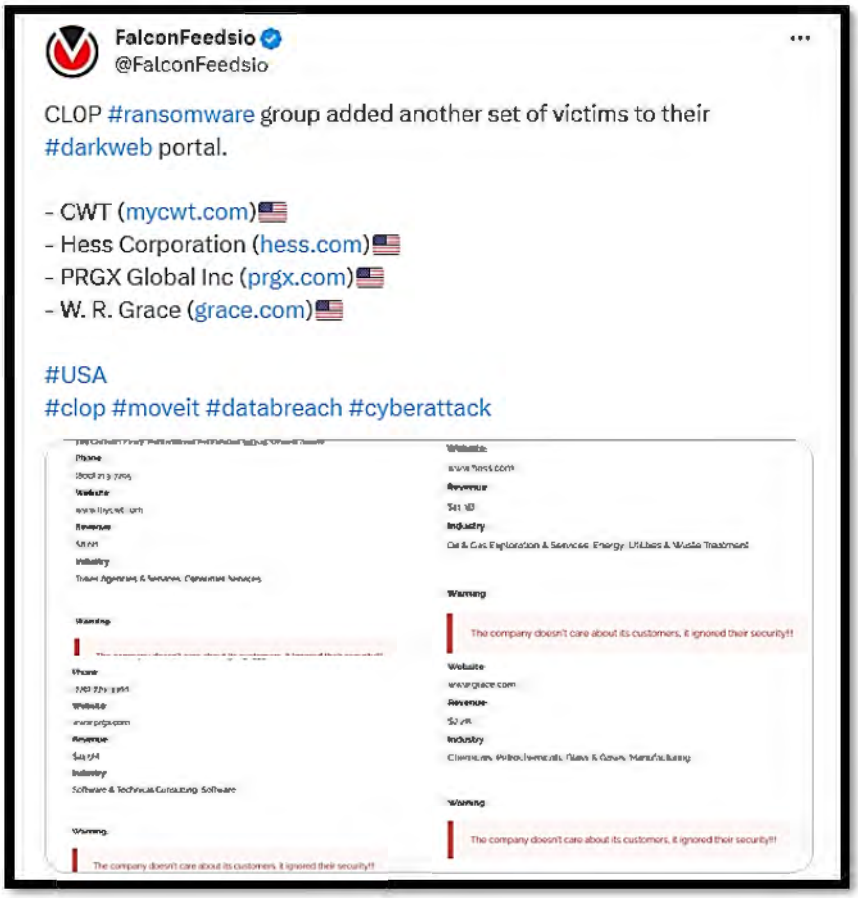
13. The Second Data Breach PRGX failed to prevent and allowed to occur was perpetrated by the criminal cybergang, Clop (the "Second Data Breach" or the "Second Breach").[10]

14. It has been reported that Clop took responsibility for the Second Data Breach on its dark web portal and stated "[t]his company doesn't care about its customers, it ignored their security!!!," as shown in the images below:[11]

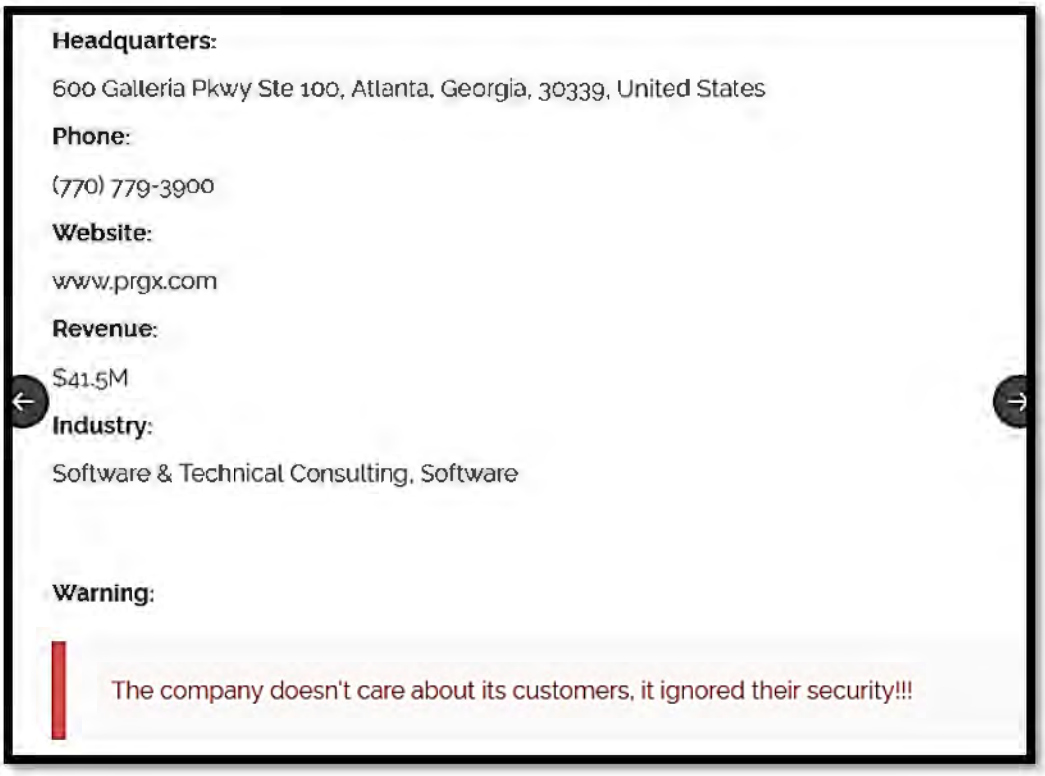
[9] *HC3 Threat Profile*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES HEALTH SECTOR CYBERSECURITY COORDINATION CENTER (Mar. 15, 2023), *available at* https://www.hhs.gov/sites/default/files/black-basta-threat-profile.pdf.

[10] *What we know about the MOVEit exploit and ransomware attacks*, BLACKFOG, https://www.blackfog.com/what-we-know-about-the-moveit-exploit/ (last visited Oct. 9, 2023).

[11] FalconFeedsio (@FalconFeedsio), TWITTER (Jul. 14, 2023, 8:25 AM), https://twitter.com/FalconFeedsio/status/1679844646325833728 (last visited Oct. 9, 2023); *see also What we know about the MOVEit exploit and ransomware attacks*, BLACKFOG, https://www.blackfog.com/what-we-know-about-the-moveit-exploit/ (last visited Oct. 9, 2023).



[ADDITIONAL IMAGE ON NEXT PAGE]

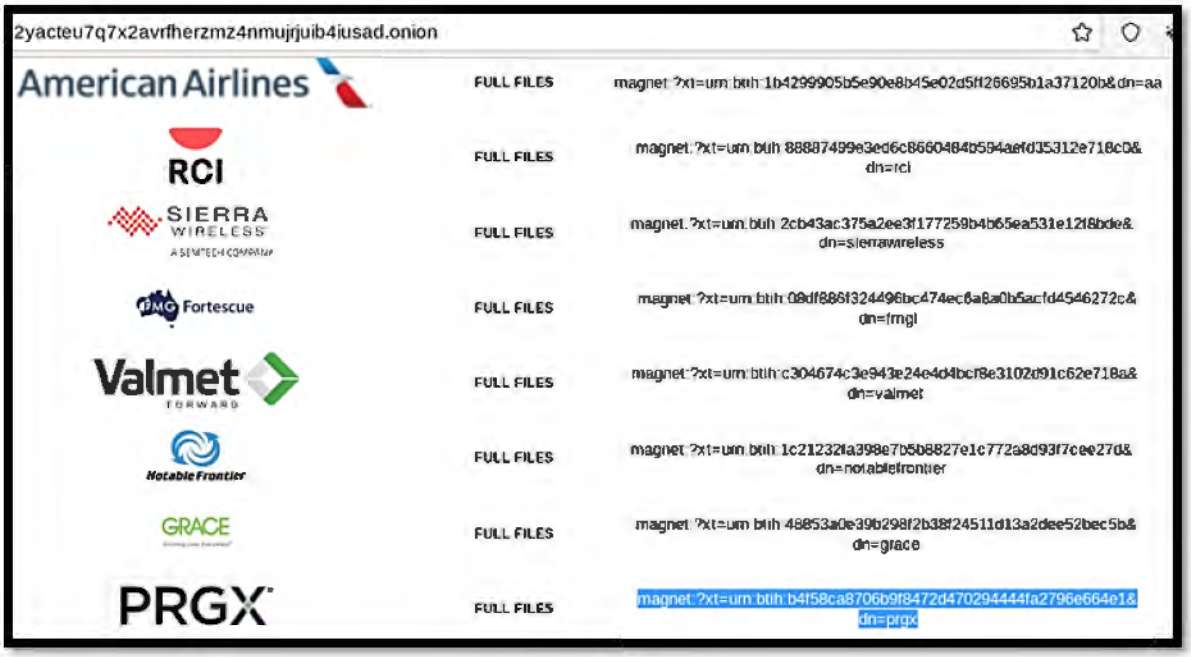


15. Like Black Basta, Clop is known for its double extortion tactics and will leak stolen PII on the dark web if the ransom demand is not paid.[12]

16. To make matters worse, ***Clop has already shared some stolen data on the dark web***:

[IMAGE ON NEXT PAGE]

[12] *See* Lawrence Abrams, *Clop ransomware now uses torrents to leak data and evade takedowns*, BLEEPINGCOMPUTER (Aug. 5, 2023, 11:16 AM), https://www.bleepingcomputer.com/news/security/clop-ransomware-now-uses-torrents-to-leak-data-and-evade-takedowns/#:~:text=Starting%20on%20May%2027th%2C%20the,they%20realized%20they%20were%20hacked (last visited Oct. 9, 2023).



17. As with the First Data Breach, PRGX has not provided Plaintiff and the Class with any assurance that it retrieved their stolen PII from Clop.

18. Plaintiffs and the Class reasonably believe their data is on the dark web and/or has already been exploited on the dark web as a result of the Data Breaches. This is specifically because: (i) PRGX failed to protect Plaintiffs' and the Class's PII, allowing two data breaches to occur; (ii) both cybergangs believed to have perpetrated the Breaches, Clop and Black Basta, stole PII and are known to leak stolen PII on the dark web, in fact Clop has already leaked some stolen data on the dark web; (iii) Defendant has not provided any assurance that it paid a ransom to the cybercriminals to prevent Plaintiffs' and the Class's data from being released on the dark web; and (iv) Defendant offered credit monitoring to Plaintiffs and the Class, an offer it need not make if no PII was stolen and at risk of misuse.

19. Due to Defendant's negligence, cybercriminals have stolen and obtained everything they need to commit identity theft and wreak havoc on the financial and personal lives of thousands of individuals.

20. Now, for the rest of their lives, Plaintiffs and the Class Members will have to deal with the danger of identity thieves possessing and misusing their PII. Even those Class Members who have yet to experience identity theft have to spend time responding to the Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiffs and Class Members have incurred and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their PII, loss of privacy, and/or additional damages as described below.

21. Plaintiffs bring this action individually and on behalf of the Class, seeking compensatory damages, punitive damages, nominal damages, restitution, and injunctive and declaratory relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

II. THE PARTIES

22. Plaintiff **Jeffrey Ebert** is an individual domiciled in Arizona. On or about May 5, 2023, Defendant sent Plaintiff Jeffrey Ebert a Notice Letter informing him that his name and Social Security number were took or viewed in the Data

Breach.

23. Plaintiff **Jennifer Ebert** is an individual domiciled in Arizona. On or about May 5, 2023, Defendant sent Plaintiff Jennifer Ebert a Notice Letter informing her that her name and Social Security number were took or viewed in the Data Breach.

24. Plaintiff Jeffrey Ebert and Plaintiff Jennifer Ebert are the parents of **minor children M.E., S.E., and E.E.** (the "Minor Plaintiffs") who also reside in Arizona. On or about May 5, 2023, Defendant sent Notice Letters "to the parent or guardian of" the Minor Plaintiffs informing them that the Minor Plaintiffs' names and Social Security numbers were took or viewed in the Data Breach.

25. Defendant **PRGX** is a Georgia corporation with its principal place of business located at 200 Galleria Pkwy, Suite 450, Atlanta, GA, 30339. Defendant maintains and transacts business across the state of Georgia.

III. JURISDICTION AND VENUE

26. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than one hundred putative Class Members, and minimal diversity exists because many putative Class Members are citizens of a different state than Defendant.

27. This Court has personal jurisdiction over Defendant because Defendant is incorporated and/or has its principal place of business in this District; conducts substantial business in this District through its headquarters, offices, and affiliates; engaged in the conduct at issue here in this District; and/or otherwise has substantial contacts with this District and purposely availed itself to the Courts in this District.

28. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District.

IV. FACTUAL ALLEGATIONS

A. PRGX and its Collection of Plaintiffs' and the Class's PII.

29. Founded in 1970, PRGX is a business services company based in Atlanta, Georgia.[13]

30. PRGX provides global recovery audit and spend analytics services and consulting services to companies in the media, banking, telecom, utilities, oil and gas, manufacturing, retail, and consumer goods industries.[14]

[13] *See PRGX Global, Inc. Notifies 13,231 Individuals of Recent Data Breach*, JDSUPRA, https://www.jdsupra.com/legalnews/prgx-global-inc-notifies-13-231-2850522/ (last visited Oct. 9, 2023).

[14] *Id.*

31. PRGX Global employs more than 1,500 people and generates approximately $41 million in annual revenue.[15]

32. PRGX could have afforded to implement adequate data security prior to the Breach but chose not to.

33. In the ordinary course of business, PRGX receives the PII of individuals, such as Plaintiffs and the Class, from the employees PRGX hires.

34. PRGX obtains, collects, uses, and derives a benefit from the PII of Plaintiffs' and Class Members. PRGX uses the PII it collects to provide services to its clients, making a profit therefrom. PRGX would not be able to obtain revenue if not for the acceptance and use of Plaintiffs' and the Class's PII.

35. By collecting Plaintiffs' and the Class's PII, PRGX assumed legal and equitable duties to Plaintiffs and the Class to protect and safeguard their PII from unauthorized access and intrusion.

36. PRGX recognizes this duty and makes the following claim on its website regarding its protection of sensitive data: "Ingesting, analyzing and storing data securely for complete privacy, control and transparency, meeting or exceeding all relevant laws, regulations and industry best practices."[16]

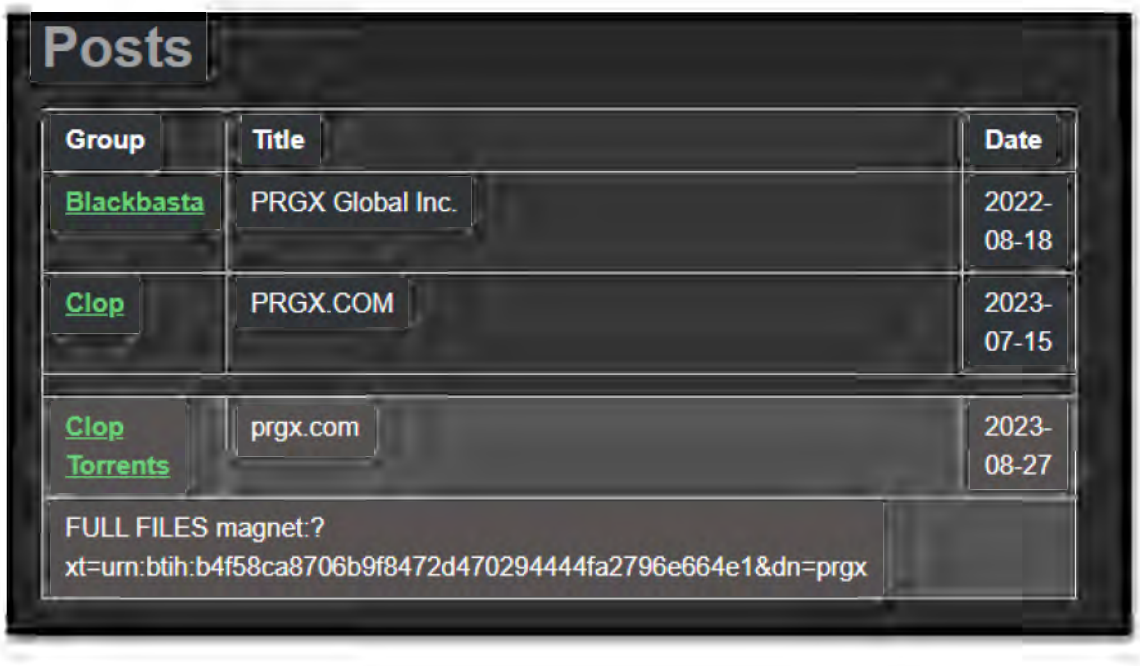
---

[15] *Id.*

[16] *See Technology Platforms*, PRGX, https://www.prgx.com/technology-platforms/ (last visited Oct. 9, 2023).

37. However, PRGX failed to protect Plaintiffs' and the Class's PII.

38. As a result, Plaintiffs' and Class Members' PII was accessed and stolen from PRGX's inadequately secured computer network in at least two data breaches, as corroborated by the source below:[17]



Posts

Group	Title	Date
Blackbasta	PRGX Global Inc.	2022-08-18
Clop	PRGX.COM	2023-07-15
Clop Torrents	prgx.com	2023-08-27
FULL FILES magnet:?xt=urn:btih:b4f58ca8706b9f8472d470294444fa2796e664e1&dn=prgx		

B. PRGX's First Data Breach.

39. On April 9, 2022, PRGX noticed that certain computer servers and systems in its environment were inaccessible.[18]

40. After an investigation, PRGX determined cybercriminals infiltrated PRGX's network and gained unauthorized access to certain files between April 8,

[17] RANSOMLOOK, https://www.ransomlook.io/search (last visited Oct. 9, 2023) (input "PRGX" in the search bar).

[18] *See* Exhibits 1–5.

2022, and April 9, 2022.[19]

41. Specifically, PRGX admits the unauthorized actor(s) "***took or viewed certain files.***"[20]

42. The PII stolen in the First Data Breach included Plaintiffs' and the Class's: (i) names; (ii) Social Security numbers; and (iii) financial information (account numbers and/or credit/debit card numbers in combination with security codes, access codes, passwords, or PINs for the accounts).[21]

43. Despite discovering the First Data Breach on April 9, 2022, PRGX took over a year to notify victims of the First Data Breach that their information was viewed and stolen, giving cybercriminals a more than a 365-day head start on misusing and exploiting Plaintiffs' and the Class's PII.

44. In recognition of the severity of the First Data Breach, and the imminent risk of impending harm Plaintiffs and the Class face, PRGX made an offering of twelve months of credit monitoring and identity restoration services through IDX to victims of the First Data Breach. Such an offering is inadequate and will not prevent

---

[19] *Id.*

[20] *Id.* (emphasis added).

[21] *See Data Breach Notifications*, OFFICE OF THE MAINE ATTORNEY GENERAL, https://apps.web.maine.gov/online/aeviewer/ME/40/f674c5b1-aad3-4c7f-84ac-422031509727.shtml (last visited Oct. 9, 2023).

identity theft but will only alert Data Breach victims once identity theft has ***already occurred***.

45. According to information and belief, victims of the First Data Breach are comprised of PRGX employees and their dependents.

46. All in all, PRGX failed to take the necessary precautions required to safeguard and protect Plaintiffs' and Class Members' PII from unauthorized access and exploitation.

47. Defendant's actions represent a flagrant disregard of the rights of Plaintiffs and the Class, both as to privacy and property.

48. Shortly after the First Data Breach, various sources reported criminal ransomware group, Black Basta, was responsible for the First Data Breach.[22]

49. Black Basta is a "financially motivated"[23] criminal ransomware group

---

[22] *See Black Basta Ransomware Victim: PRGX Global Inc[.]*, REDPACKET SECURITY, https://www.redpacketsecurity.com/black-basta-ransomware-victim-prgx-global-inc/ (last visited Oct. 9, 2023); *Weekly Dark Web Trends/Advisory*, CYFIRMA, *available at* https://www.prianto.com/fileadmin/user_upload/PRIANTO_CEE/Cyfirma/Weekly_Dark_Web_Trends_and_Advisory_13_May_2022.pdf (last visited Oct. 9, 2023); *Profiles for ransomware group: blackbasta*, RANSWOMWARE.LIVE, https://www.ransomware.live/#/group/blackbasta (last visited Oct. 9, 2023); RANSOMLOOK, https://www.ransomlook.io/search (input "PRGX" in the search bar) (last visited Oct. 9, 2023).

[23] *HC3 Threat Profile*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES HEALTH SECTOR CYBERSECURITY COORDINATION CENTER (Mar. 15, 2023), *available at* https://www.hhs.gov/sites/default/files/black-basta-threat-profile.pdf.

who is "aggressive and highly active."[24]

50. Black Basta is "known for its double extortion attack"[25] and has "proven itself to be a formidable threat."[26]

51. Like other ransomware gangs, Black Basta ***steals*** corporate data and documents before it encrypts the information.[27]

52. "Once the encryption process is complete, the malware changes the wallpaper, and files on the desktop become encrypted and unusable," as pictured below:[28]

---

[24] *Black Basta, Anatomy of the Attack*, INFOBLOX (May 19, 2023) https://blogs.infoblox.com/cyber-threat-intelligence/black-basta-anatomy-of-the-attack/ (last visited Oct. 9, 2023).

[25] *HC3 Threat Profile*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES HEALTH SECTOR CYBERSECURITY COORDINATION CENTER (Mar. 15, 2023), *available at* https://www.hhs.gov/sites/default/files/black-basta-threat-profile.pdf.

[26] *Ransomware Spotlight Black Basta*, TREND MICRO INCORPORATED (Sept. 1, 2022), https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta (last visited Oct. 9, 2023).

[27] Lawrence Abrams, *New Black Basta ransomware spring into action with a dozen breaches*, BLEEPINGCOMPUTER (April 27, 2022, 5:46 PM), https://www.bleepingcomputer.com/news/security/new-black-basta-ransomware-springs-into-action-with-a-dozen-breaches/ (last visited Oct. 9, 2023)

[28] *HC3 Threat Profile*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES HEALTH SECTOR CYBERSECURITY COORDINATION CENTER (Mar. 15, 2023), *available at* https://www.hhs.gov/sites/default/files/black-basta-threat-profile.pdf; Lawrence Abrams, *New Black Basta ransomware spring into action with a dozen breaches*, BLEEPINGCOMPUTER (April 27, 2022, 5:46 PM),

Wallpaper added by the Black Basta encryptor
Source: BleepingComputer

53. Black Basta then demands a hefty ransom from the company it steals the information from in exchange for a decryptor, which will allow the company to access its files again.[29]

54. Below is the ransom note Black Basta typically uses:[30]

[IMAGE ON NEXT PAGE]

---

https://www.bleepingcomputer.com/news/security/new-black-basta-ransomware-springs-into-action-with-a-dozen-breaches/ (last visited Oct. 9, 2023).

[29] Lawrence Abrams, *New Black Basta ransomware spring into action with a dozen breaches*, BLEEPINGCOMPUTER (April 27, 2022, 5:46 PM), https://www.bleepingcomputer.com/news/security/new-black-basta-ransomware-springs-into-action-with-a-dozen-breaches/ (last visited Oct. 9, 2023).

[30] *Id.*

Black Basta Ransom Note

Source: BleepingComputer

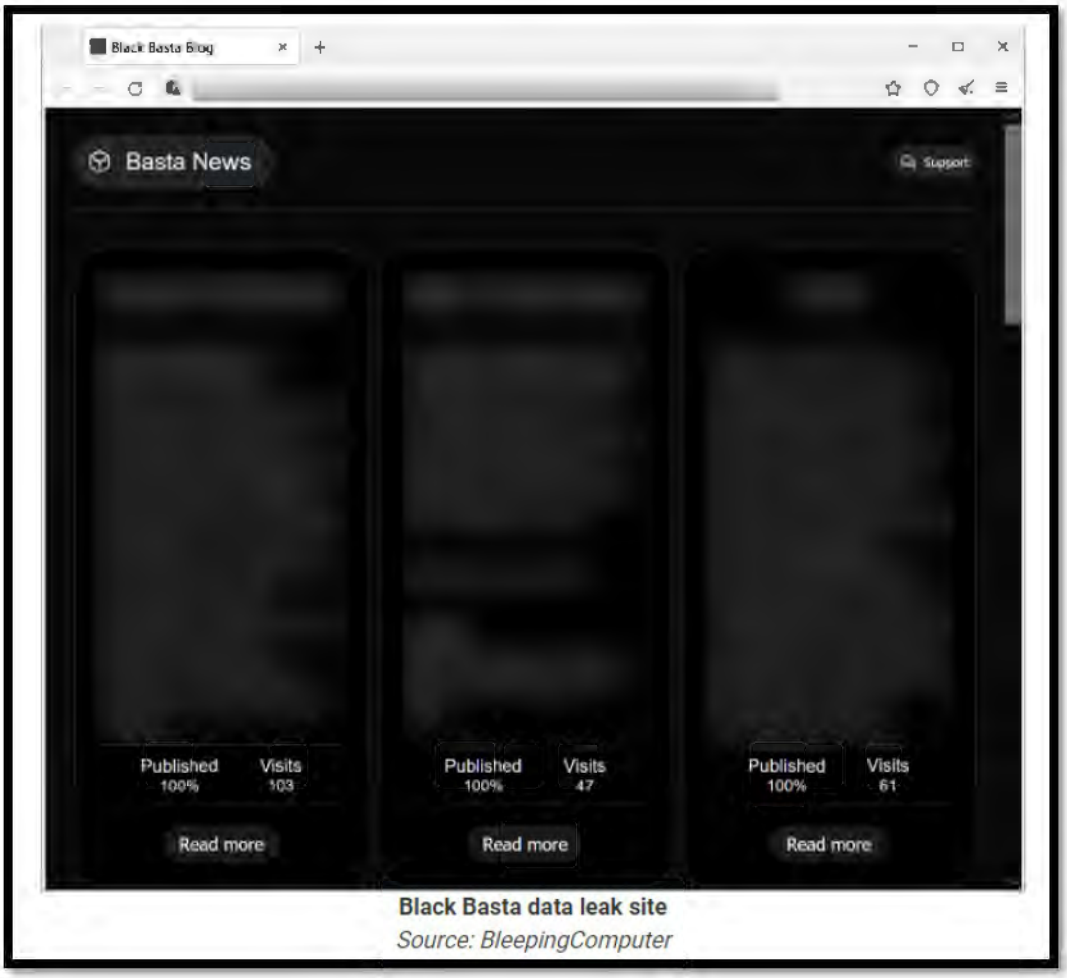
55. Black Basta "not only executes ransomware, but also exfiltrates sensitive data, operating a cybercrime marketplace to publicly release it, should a victim fail to pay a ransom."[31]

56. Black Basta "deploys a name-and-shame approach to their victims, using a Tor site, Basta News, to publicly list victims' names, descriptions, percentage of published data stolen, number of visits, and any other data exfilrated [sic].[32]

[IMAGE ON NEXT PAGE]

[31] *HC3 Threat Profile*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES HEALTH SECTOR CYBERSECURITY COORDINATION CENTER (Mar. 15, 2023), *available at* https://www.hhs.gov/sites/default/files/black-basta-threat-profile.pdf.

[32] *Id.*; Amer Elsad, *Threat Assessment: Black Basta Ransomware*, UNIT 42 (Aug. 25, 2022 12:00 PM) https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware/ (last visited Oct. 9, 2023).



Black Basta data leak site

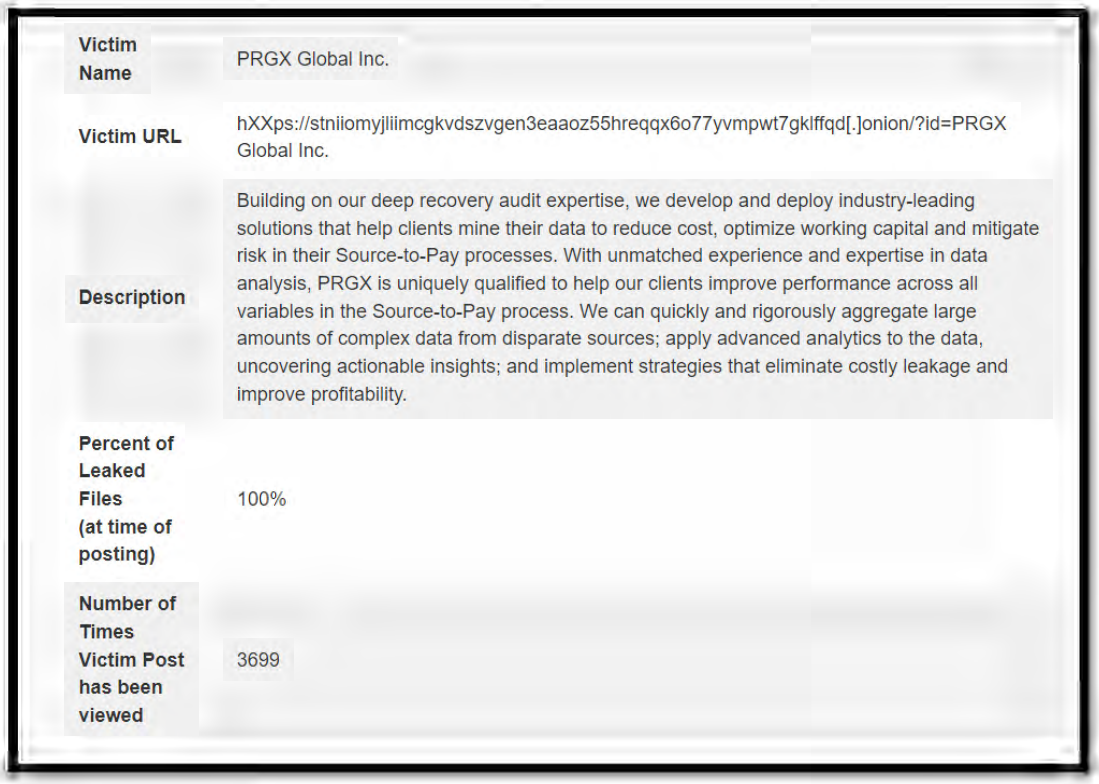
Source: BleepingComputer

57. "Black Basta will slowly leak data for each victim to try and pressure them into paying a ransom."[33]

58. As evidenced below, a source claims Black Basta already deployed its

[33] Lawrence Abrams, *New Black Basta ransomware spring into action with a dozen breaches*, BLEEPINGCOMPUTER (April 27, 2022, 5:46 PM), https://www.bleepingcomputer.com/news/security/new-black-basta-ransomware-springs-into-action-with-a-dozen-breaches/ (last visited Oct. 9, 2023)

signature approach here:[34]



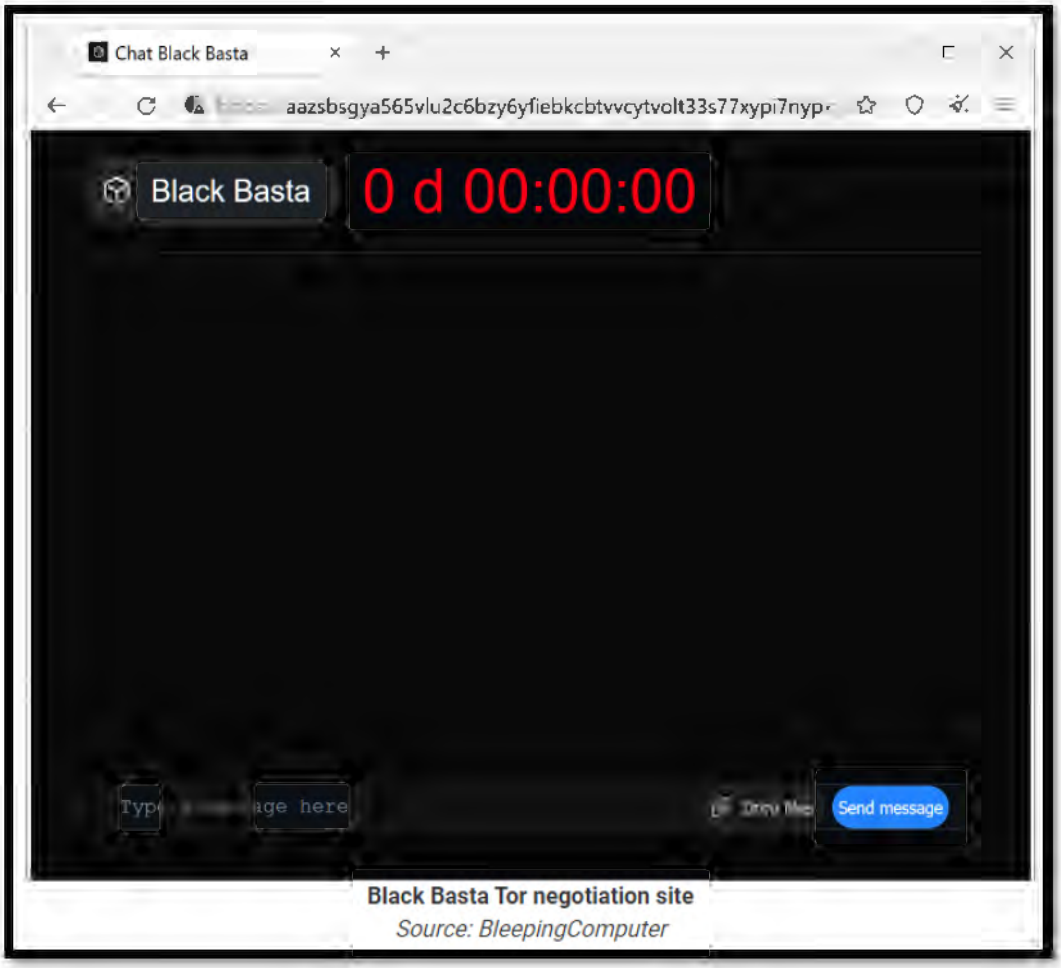
Victim Name	PRGX Global Inc.
Victim URL	hXXps://stniiomyjliimcgkvdszvgen3eaaoz55hreqqx6o77yvmpwt7gklffqd[.]onion/?id=PRGX Global Inc.
Description	Building on our deep recovery audit expertise, we develop and deploy industry-leading solutions that help clients mine their data to reduce cost, optimize working capital and mitigate risk in their Source-to-Pay processes. With unmatched experience and expertise in data analysis, PRGX is uniquely qualified to help our clients improve performance across all variables in the Source-to-Pay process. We can quickly and rigorously aggregate large amounts of complex data from disparate sources; apply advanced analytics to the data, uncovering actionable insights; and implement strategies that eliminate costly leakage and improve profitability.
Percent of Leaked Files (at time of posting)	100%
Number of Times Victim Post has been viewed	3699

59. Black Basta will leak the data it steals if the ransom demand is not paid:[35]

[IMAGE ON NEXT PAGE]

[34] *See Black Basta Ransomware Victim: PRGX Global Inc[.]*, REDPACKET SECURITY, https://www.redpacketsecurity.com/black-basta-ransomware-victim-prgx-global-inc/ (last visited Oct. 9, 2023) (reporting dark web findings).

[35] *See* Lawrence Abrams, *New Black Basta ransomware spring into action with a dozen breaches*, BLEEPINGCOMPUTER (April 27, 2022, 5:46 PM), https://www.bleepingcomputer.com/news/security/new-black-basta-ransomware-springs-into-action-with-a-dozen-breaches/ (last visited Oct. 9, 2023); *Weekly Dark Web Trends/Advisory*, CYFIRMA, *available at* https://www.prianto.com/fileadmin/user_upload/PRIANTO_CEE/Cyfirma/Weekly_Dark_Web_Trends_and_Advisory_13_May_2022.pdf (last visited Oct. 9, 2023).



Black Basta Tor negotiation site

Source: BleepingComputer

60. PRGX makes ***no*** assurances to Plaintiffs and the Class that it attempted to regain Plaintiffs' and the Class's data from Black Basta, paid the ransom demand, or that their data has not already been posted on the dark web.

61. Even if PRGX did pay the ransom this does not mean that Black Basta will not exploit Plaintiffs' and the Class's PII in the future for further financial gain or has not already done so. After all, Black Basta is a "financially motivated" group

of criminals.[36]

C. PRGX's Second Data Breach.

62. Even after the First Data Breach, PRGX still failed to take data security seriously.

63. In fact, after the First Data Breach, PRGX experienced ***another*** data breach perpetrated by a different cybergang, Clop.[37]

64. According to FalconFeeds.io, Clop added PRGX as a victim to its dark web portal on or around July 14, 2023:[38]

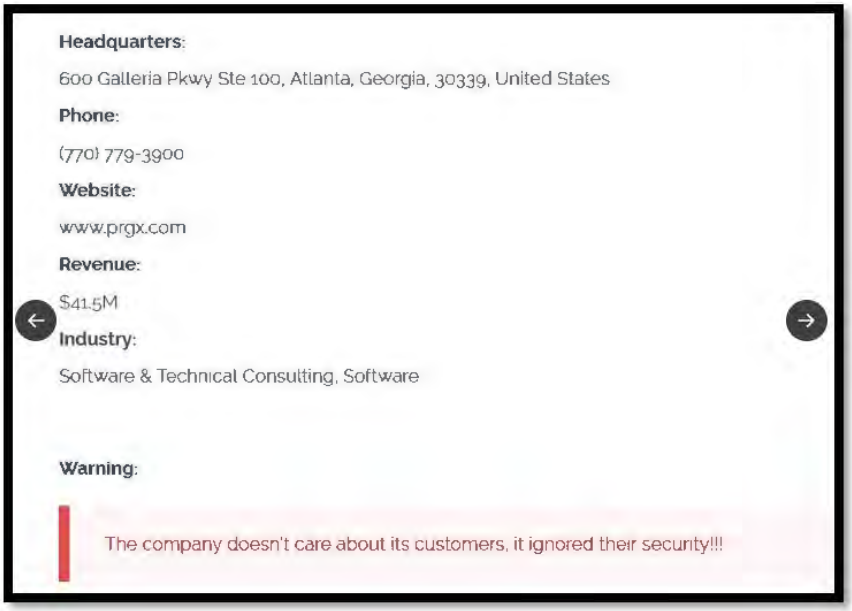
[IMAGE ON NEXT PAGE]

---

[36] *HC3 Threat Profile*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES HEALTH SECTOR CYBERSECURITY COORDINATION CENTER (Mar. 15, 2023) *available at* https://www.hhs.gov/sites/default/files/black-basta-threat-profile.pdf.

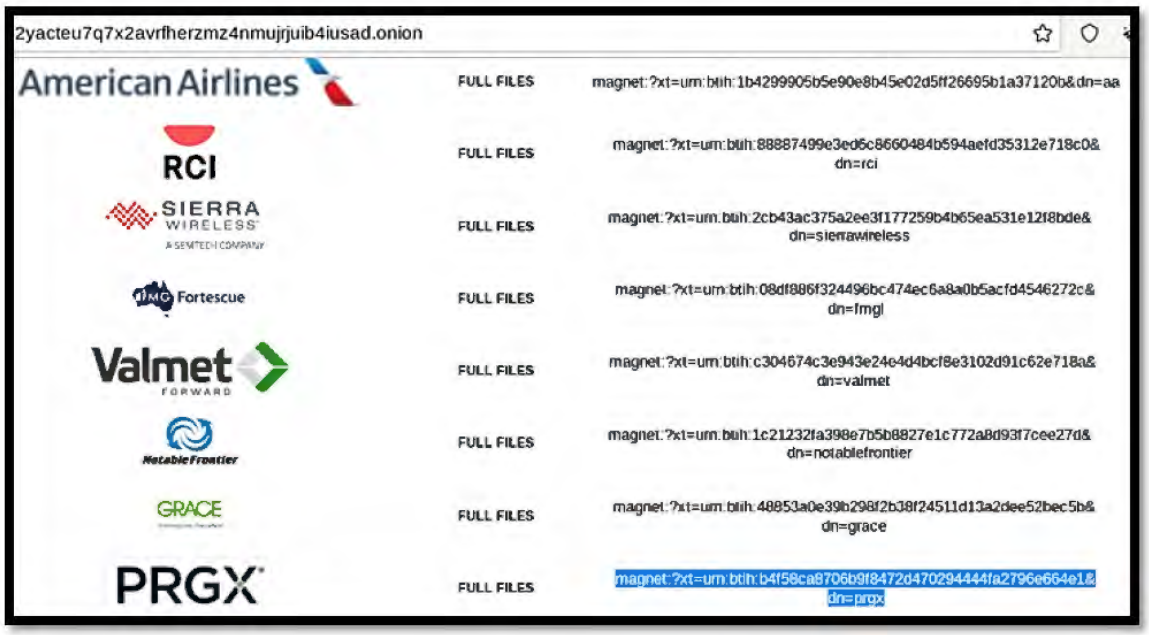
[37] FalconFeedsio (@FalconFeedsio), TWITTER (Jul. 14, 2023, 8:25 AM), https://twitter.com/FalconFeedsio/status/1679844646325833728 (last visited Oct. 9, 2023) (reporting the victims Clop added to its dark web portal); *What we know about the MOVEit exploit and ransomware attacks*, BLACKFOG, https://www.blackfog.com/what-we-know-about-the-moveit-exploit/.

[38] FalconFeedsio (@FalconFeedsio), TWITTER (Jul. 14, 2023, 8:25 AM), https://twitter.com/FalconFeedsio/status/1679844646325833728 (last visited Oct. 9, 2023).



65. PRGX has yet to disclose the details of the full extent of the Second Data Breach, including how many individuals had their data stolen, what information was stolen, and if it paid a ransom demand.

66. However, Clop has already shared some stolen data on the dark web:



67. Clop is also known to leak stolen data on the clear web.[39]

68. All in all, PRGX has left Plaintiffs and the Class in the dark with respect to both Data Breaches.

69. Plaintiffs and the Class reasonably believe their data is on the dark web or has already been sold/exploited on the dark web because: (i) PRGX failed to prevent two data breaches; (ii) both cybergangs believed to have perpetrated the Breaches, Clop and Black Basta, are known to leak stolen PII on the dark web and indeed, Clop has already shared some stolen data on the dark web; (iii) Defendant has not provided any assurance that it paid a ransom to the cybercriminals to prevent Plaintiffs' and the Class's data from being released on the dark web; and (iv) Defendant offered credit monitoring to Plaintiffs and the Class, an offer it need not make if no PII was stolen and at risk of misuse.

D. Cyber Criminals Have Used and Will Continue to Use Plaintiffs' and the Class's PII to Defraud Them.

70. PII is of great value to hackers and cybercriminals, and the data stolen in the Data Breaches can and will be used in a variety of ways by criminals to exploit Plaintiffs and the Class Members and to profit off their misfortune.

---

[39] Lawrence Abrams, *Clop now leaks data stolen in MOVEit attacks on clearweb sites*, BLEEPINGCOMPUTER (Jul. 23, 2023, 3:10 PM), https://www.bleepingcomputer.com/news/security/clop-now-leaks-data-stolen-in-moveit-attacks-on-clearweb-sites/#:~:text=Clop%20ransomware%20gang%20adopts%20tactic,MOVEit%20Transfer%20data%20theft%20attacks.

71. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[40]

72. For example, with the PII stolen in the Data Breaches, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[41] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and the Class Members.

73. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number.** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal

---

[40] *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity") (last visited Oct. 9, 2023).

[41] *See, e.g.*, Christine DiGangi, *What Can You Do with a Stolen Social Security Number*, CREDIT.COM (June 29, 2020), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (last visited Oct. 9, 2023).

> matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[42]
>
> [Emphasis added.]

74. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.[43]

75. These were a financially motivated Breaches, as the only reason the cyber criminals go through the trouble of running targeted cyberattacks against companies like PRGX is to get ransom money and/or information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein.

76. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[44]

---

[42] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/ (last visited Oct. 9, 2023).

[43] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, available at https://www.gao.gov/products/gao-07-737.

[44] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web* (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web (last visited Oct. 9, 2023).

77. "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[45]

78. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if hackers get access to PII, ***they will use it***.[46]

79. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n 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.[47]

---

[45] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/ (last visited Oct. 9, 2023).

[46] Ari Lazarus, *How fast will identity thieves use stolen info?*, MILITARY CONSUMER (May 24, 2017), https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info (last visited Oct. 9, 2023).

[47] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,* GAO (July 5, 2007), available at https://www.gao.gov/products/gao-07-737.

80. For instance, with a stolen social security number, which is part of the PII compromised in the Data Breaches, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[48]

81. With these Data Breaches, identity thieves have already started to prey on the PRGX breach victims, and we can anticipate that this will continue.

82. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[49]

83. Defendant's offer of one year of identity monitoring to Plaintiffs and the Class is woefully inadequate and will not fully protect Plaintiffs from the damages and harm caused by its failures.

84. The full scope of the harm has yet to be realized. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used.

---

[48] *See, e.g.*, Christine DiGangi, *What Can You Do with a Stolen Social Security Number*, CREDIT.COM (June 29, 2020), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (last visited Oct. 9, 2023).

[49] *Guide for Assisting Identity Theft Victims*, FEDERAL TRADE COMMISSION (Sept. 2013), *available at* https://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf.

85. Once the twelve-months have expired, Plaintiffs and Class Members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives due to PRGX's gross negligence.

86. Furthermore, identity monitoring only alerts someone to the fact that they have ***already been the victim of identity theft*** (*i.e.*, fraudulent acquisition and use of another person's PII)—it does not prevent identity theft.[50] Nor can an identity monitoring service remove personal information from the dark web.[51]

87. "The people who trade in stolen personal information [on the dark web] won't cooperate with an identity theft service or anyone else, so it's impossible to get the information removed, stop its sale, or prevent someone who buys it from using it."[52]

88. As a direct and proximate result of the Data Breaches Plaintiffs and the Class have been damaged and have been placed at an imminent, immediate, and continuing increased risk of harm from continued fraud and identity theft. Plaintiffs and the Class must now take the time and effort to mitigate the actual and potential

---

[50] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017, 9:00 AM), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html (last visited Oct. 9, 2023).

[51] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/ (last visited Oct. 9, 2023).

[52] *Id.*

impact of the Data Breaches 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.

89. Even more seriously is the identity restoration that Plaintiffs and other Class Members must go through, which can include spending countless hours filing police reports, filling out IRS forms, Federal Trade Commission checklists, Department of Motor Vehicle driver's license replacement applications, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps Plaintiffs and the Class must take.

90. Plaintiffs and the Class have or will experience the following concrete and particularized harms for which they are entitled to compensation, including:

a. Actual identity theft;

b. Trespass, damage to, and theft of their personal property including PII;

c. Improper disclosure of their PII;

d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

e. Loss of privacy suffered as a result of the Data Breaches, including the harm of knowing cyber criminals have their PII;

f. Ascertainable losses in the form of time taken to respond to identity theft and attempt to restore identity, including lost opportunities and lost wages from uncompensated time off from work;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breaches;

h. Ascertainable losses in the form of deprivation of the value of Plaintiffs' and Class members' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their PII; and/or

k. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

91. Moreover, Plaintiffs and Class Members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard security measures and safeguards. Defendant has shown itself wholly incapable of protecting Plaintiffs' PII.

92. Plaintiffs and Class Members also have an interest in ensuring that their personal information that was provided to PRGX is removed from all PRGX servers, systems, and files.

93. Defendant itself acknowledged the harm caused by the First Data Breach because it offered Plaintiffs and Class Members the woefully inadequate twelve months of identity theft repair and monitoring services. Twelve months of identity theft and repair and monitoring is, however, inadequate to protect Plaintiffs and Class Members from a lifetime of identity theft risk.

94. Defendant further acknowledged, in its letter to Plaintiffs and other Class Members, that PRGX needed to improve its security protocols, stating: "while we have safeguards in place to protect data in our care, we have taken steps to further enhance these protections and continue to monitor these safeguards as part of our ongoing commitment to data security."[53] These enhanced protections should have been in place before the First Data Breach.

95. The letter further acknowledged that the First Data Breach would cause inconvenience to affected individuals and that financial harm would likely occur, stating: "We encourage you to remain vigilant against incidents of identity theft and

[53] *See* Exhibits 1–5.

fraud by reviewing your account statements and monitoring your credit reports for suspicious activity and to detect errors."[54]

96. At PRGX's suggestion, Plaintiffs are desperately trying to mitigate the damage that PRGX has caused them.

97. Given the kind of PII PRGX made accessible to hackers, however, Plaintiffs are certain to incur additional damages. Because identity thieves have their PII, Plaintiffs and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[55]

98. None of this should have happened because the Data Breaches were entirely preventable.

E. Defendant was Aware of the Risk of Cyberattacks.

99. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can

---

[54] *Id.*

[55] *What happens if I change my Social Security number*, LEXINGTON LAW (Aug. 10, 2022), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html (last visited Oct. 9, 2023).

tell you the names of some of the biggest cybersecurity breaches: Target,[56] Yahoo,[57] Marriott International,[58] Chipotle, Chili's, Arby's,[59] and others.[60]

100. PRGX should certainly have been aware, and indeed was aware, that it was at risk of a data breach that could expose the PII that it collected and maintained, especially after the First Data Breach.

101. Indeed, PRGX's Privacy Policy[61] states in pertinent part as follows:

---

[56] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/ (last visited Oct. 9, 2023).

[57] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html (last visited Oct. 9, 2023).

[58] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/ (last visited Oct. 9, 2023).

[59] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018, 12:58 PM), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b (last visited Oct. 9, 2023).

[60] *See, e.g.*, Michael Hill and Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Nov. 8, 2022), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html (last visited Oct. 9, 2023).

[61] *Privacy Statement*, PRGX, https://www.prgx.com/privacy-policy/#:~:text=PRGX%20is%20committed%20to%20protecting,internal%20policies%2C%20practices%20and%20procedures (last visited Oct. 9, 2023).

How We Protect Personal Information We Process on Behalf of Our Clients

PRGX is a business-to-business information and professional services firm that collects and processes transactional client data for improving clients' financial performance by reducing costs, improving business processes and increasing profitability. PRGX's core business segment is recovery audit services which is the processing of source-to-pay transactional information (e.g., accounts payable data, vendor file information and line item/product data) to identify client overpayments made to their third-party suppliers or vendors. Other business segments include providing analytics and advisory services to senior financial executives.

We process this transactional information on behalf of our clients to perform the requested services. This transactional information may contain Personal Information in limited circumstances, such as when a client's third-party supplier or vendor happens to be a sole proprietor. Information on these individuals is used and processed as instructed by our clients for accounts payable recovery auditing or other requested services in accordance with client contractual requirements. In any event, regarding transactional information that constitutes Personal Information, we act in a data processor capacity, meaning we collect and process this Personal Information only as instructed by our client and will not use or disclose it for our own purposes.

We do, however, maintain information security controls to protect this Personal Information and will only disclose or transfer this information as instructed by or agreed upon with our client to provide the requested service. Unless otherwise instructed by our clients, we treat the Personal Information we process on behalf of our clients in line

with our commitments on disclosure and transfer as set forth in this Statement.

* * *

Security And Data Integrity

PRGX is committed to protecting the privacy, confidentiality, and security of the data that is provided to us, including Personal Information, through a combination of technical, physical and administrative controls, including internal policies, practices and procedures.

We apply appropriate technical, physical and organizational measures that are reasonably designed to protect Personal Information against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access where Personal Information is transferred over a network, and against all other unlawful forms of processing. Access to Personal Information is restricted to authorized recipients on a need-to-know basis. We maintain a comprehensive information security program that is proportionate to the risks associated with the processing. The program is continuously adapted to mitigate operational risks and to ensure the protection of Personal Information taking into account industry-accepted practices. We will also use enhanced security measures in case we process any Sensitive Personal Information.

PRGX's privacy and security framework is based on ISO 27001 standards and, as such, we have a strong focus on establishing, maintaining, and continuously improving information security management systems and identifying, analyzing, and addressing information security risks. The ISO 27001 standards cover all aspects of security including physical protection of equipment and

> people, hiring practices, employee training, network security, and access controls. This framework combined with regular monitoring and testing of controls, allows us to ensure that appropriate levels of data confidentiality, integrity, and availability are maintained.

102. PRGX's assurances of maintaining high standards of cybersecurity make it evident that PRGX recognized it had a duty to use reasonable measures to protect the PII that it collected and maintained.

103. PRGX was clearly aware of the risks it was taking and the harm that could result from inadequate data security.

F. PRGX Could Have Prevented the Data Breaches.

104. Data breaches are preventable.[62] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[63] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[64]

---

[62] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012), available at https://lawcat.berkeley.edu/record/394088.

[63] *Id.* at 17.

[64] *Id.* at 28.

105. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[65]

106. In Data Breaches like these, many failures laid the groundwork for the Breach.

107. The FTC has published guidelines that establish reasonable data security practices for businesses.

108. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[66]

109. The FTC guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks;

---

[65] *Id.*

[66] *Protecting Personal Information: A Guide for Business*, FTC, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems.

110. The FTC guidelines also recommend that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

111. According to information and belief, PRGX failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines.

112. Upon information and belief, PRGX also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity readiness.

113. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[67]

114. To prevent and detect malware attacks, including the malware attack that resulted in the Data Breaches, Defendant could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

[67] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs 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.[68]

115. Further, to prevent and detect malware attacks, including the malware attacks that resulted in the Data Breaches, 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.

[68] *Id.* at 3–4.

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 for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[69]

116. In addition, to prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breaches, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

[69] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), available at https://www.cisa.gov/news-events/news/protecting-against-ransomware.

- **Secure internet-facing assets**
  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privileged credentials
- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as potential full compromise;
- **Include IT Pros in security discussions**
  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
- **Build credential hygiene**
  - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
- **Apply principle of least-privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events

- **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].[70]

117. Given that Defendant was storing the PII of more than 13,000 individuals, Defendant could have and should have implemented all of the above measures to prevent and detect cyberattacks.

118. Specifically, among other failures, PRGX had far too much confidential unencrypted information held on its systems. Such PII should have been segregated into an encrypted system.[71]

119. Moreover, it is well-established industry standard practice for a business to dispose of confidential PII once it is no longer needed.

---

[70] *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/.

[71] *See, e.g.,* Adnan Raja, *How to Safeguard Your Business Data with Encryption*, FORTRA (Aug. 14, 2018), https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption (last visited Oct. 9, 2023).

120. The FTC, among others, has repeatedly emphasized the importance of disposing unnecessary PII, saying simply: "Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it's not on your system, it can't be stolen by hackers."[72] PRGX, rather than following this basic standard of care, kept thousands of individuals' unencrypted PII indefinitely.

121. In sum, these Data Breaches could have readily been prevented through the use of industry standard network segmentation and encryption of all PII.

122. Further, the scope of the Data Breaches could have been dramatically reduced had PRGX utilized proper record retention and destruction practices.

G. Plaintiffs' Individual Experiences

Plaintiff Jeffrey Ebert's Experience and the Minor Plaintiffs' Experiences

123. Plaintiff Jeffrey Ebert is a former employee of Defendant. Plaintiff agreed to entrust his PII and the Minor Plaintiffs' PII to Defendant as a condition of receiving employment and/or elective benefits. In exchange, Defendant agreed not only to accept this PII, but also to safeguard it and delete it after a reasonable time following the termination of the employment relationship. Plaintiff Jeffrey Ebert did not reasonably expect that he was providing his and the Minor Plaintiffs' PII to

[72] *Protecting Personal Information: A Guide for Business*, FTC, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf, at p. 6.

Defendant forever.

124. Defendant was in possession of Plaintiff Jeffrey Ebert's PII and the Minor Plaintiffs' PII before, during, and after the Data Breaches.

125. In or around May 2023, Plaintiff Jeffrey Ebert and the Minor Plaintiffs received Notice Letters from Defendant informing them that they were victims of the First Data Breach and that an unauthorized actor "took or viewed certain files" in the First Data Breach, including their PII.

126. Due to the proximity of the First and Second Data Breaches, the fact PRGX has failed to protect their PII once, and the fact that PRGX has provided no assurance their PII has since been deleted off of PRGX's systems, Plaintiff Jeffrey Ebert reasonably believes that his and the Minor Plaintiffs' PII was also stolen in the Second Data Breach.

127. As a direct and traceable result of the Data Breaches, Plaintiff Jeffrey Ebert has been forced to spend time dealing with and responding to the direct consequences of the Data Breaches, which includes researching the Data Breaches, reviewing, and monitoring his accounts for fraudulent activity, reviewing his credit reports, and/or researching credit monitoring services. However, this is not the end. Plaintiff Jeffrey Ebert, the Minor Plaintiffs, and Class Members will be forced to expend additional time to review their credit reports and monitor their accounts for the rest of their lives. This is time spent at Defendant's direction, which has been

lost forever and cannot be recaptured.

128. Plaintiff Jeffrey Ebert and the Minor Plaintiffs place significant value in the security of their PII and do not readily disclose it. Plaintiff Jeffrey Ebert entrusted his PII and the Minor Plaintiffs' PII to Defendant with the understanding that Defendant would keep this information secure and would employ reasonable and adequate security measures to ensure that their PII would not be compromised.

129. Plaintiff Jeffrey Ebert and the Minor Plaintiffs have never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

130. As a direct and traceable result of the Data Breaches, Plaintiff Jeffrey Ebert and the Minor Plaintiffs suffered actual damages such as: (1) lost time related to monitoring their accounts and credit reports for fraudulent activity; (2) loss of privacy due to their PII being accessed by cybercriminals; (3) loss of the benefit of the bargain because Defendant did not adequately protect their PII; (4) emotional distress because identity thieves now possess their first and last name paired with their Social Security numbers; (5) exposure to increased and imminent risk of fraud and identity theft now that their PII has been accessed; (6) the loss in value of their PII due to their PII being in the hands of cybercriminals who can use it at their leisure; and/or (7) other economic and non-economic harm.

131. Plaintiff Jeffrey Ebert and the Minor Plaintiffs have been and will continue to be at a heightened and substantial risk of future identity theft and its

attendant damages for ***years*** to come, especially the Minor Plaintiffs. Such a risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breaches. Indeed, Defendant acknowledged the increased risk of future harm Plaintiffs and the Class now face by offering complimentary credit monitoring services to Plaintiffs and the Class.

132. Knowing that thieves intentionally targeted and stole his and the minor Plaintiffs' PII, including their Social Security numbers, and knowing that their PII is in the hands of cybercriminals has caused great anxiety beyond mere worry. Specifically, Plaintiff Jeffrey Ebert has lost hours of sleep, is in a constant state of stress, is very frustrated, and is in a state of persistent worry now that his PII and the Minor Plaintiffs' PII has been stolen.

133. Plaintiff Jeffrey Ebert and the Minor Plaintiffs have a continuing interest in ensuring that their PII, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiffs', and the Class's PII will be wholly unprotected and at-risk of future data breaches.

Plaintiff Jennifer Ebert's Experience

134. Plaintiff Jennifer Ebert is the spouse of Jeffrey Ebert, and the mother of the Minor Plaintiffs. Plaintiff agreed to entrust her PII to Defendant to receive elective benefits stemming from her husband's employment with PRGX. In

exchange, Defendant agreed not only to accept her PII, but also to safeguard it and delete it after a reasonable time following the termination of the employment relationship with Jeffrey Ebert. Plaintiff Jennifer Ebert did not reasonably expect that she was providing her PII to Defendant forever.

135. Defendant was in possession of Plaintiff Jennifer Ebert's PII before, during, and after the Data Breaches.

136. In or around May 2023, Plaintiff Jennifer Ebert received a Notice Letter from Defendant informing her that she was a victim of the First Data Breach and that an unauthorized actor "took or viewed certain files" in the First Data Breach, which included her PII.

137. Due to the proximity of the First and Second Data Breaches, the fact PRGX has failed to protect her PII once, and the fact that PRGX has provided no assurance her PII has since been deleted off of PRGX's systems, Plaintiff Jennifer Ebert reasonably believes that her PII was also stolen in the Second Data Breach.

138. As a direct and traceable result of the Data Breaches, Plaintiff Jennifer Ebert has been forced to spend time dealing with and responding to the direct consequences of the Data Breaches, which includes researching the Data Breaches, reviewing, and monitoring her accounts for fraudulent activity, reviewing her credit reports, and/or researching credit monitoring services. However, this is not the end. Plaintiff Jennifer Ebert and Class Members will be forced to expend additional time

to review their credit reports and monitor their accounts for the rest of their lives. This is time spent at Defendant's direction, which has been lost forever and cannot be recaptured.

139. Plaintiff Jennifer Ebert places significant value in the security of her PII and does not readily disclose it. Plaintiff Jennifer Ebert entrusted her PII to Defendant with the understanding that Defendant would keep her information secure and would employ reasonable and adequate security measures to ensure that her PII would not be compromised.

140. Plaintiff Jennifer Ebert has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

141. As a direct and traceable result of the Data Breaches, Plaintiff Jennifer Ebert suffered actual damages such as: (1) lost time related to monitoring her accounts and credit reports for fraudulent activity; (2) loss of privacy due to her PII being accessed by cybercriminals; (3) loss of the benefit of the bargain because Defendant did not adequately protect her PII; (4) emotional distress because identity thieves now possess her first and last name paired with her Social Security number; (5) exposure to increased and imminent risk of fraud and identity theft now that her PII has been accessed; (6) the loss in value of her PII due to her PII being in the hands of cybercriminals who can use it at their leisure; and (7) other economic and non-economic harm.

142. Plaintiff Jennifer Ebert has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for ***years*** to come. Such a risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breaches. Indeed, Defendant acknowledged the increased risk of future harm Plaintiffs and the Class now face by offering complimentary credit monitoring services to Plaintiffs and the Class.

143. Knowing that thieves intentionally targeted and stole her PII, including her and the Minor Plaintiffs' Social Security numbers, and knowing that their PII is in the hands of cybercriminals has caused Plaintiff Jennifer Ebert great anxiety beyond mere worry. Specifically, Plaintiff Jennifer Ebert has lost hours of sleep, is in a constant state of stress, is very frustrated, and is in a state of persistent worry now that her and the Minor Plaintiffs' PII has been stolen.

144. Plaintiff Jennifer Ebert has a continuing interest in ensuring that her PII, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiffs', and the Class's PII will be wholly unprotected and at-risk of future data breaches.

V. CLASS ACTION ALLEGATIONS

145. Plaintiffs incorporate by reference all preceding paragraphs as if fully restated here.

146. Plaintiffs bring this action against PRGX on behalf of themselves and all other individuals similarly situated under Federal Rule of Civil Procedure 23. Plaintiffs assert all claims on behalf of a nationwide class (the "Class") defined as follows:

> **All persons whose PII was compromised due to data breaches experienced by PRGX from April 2022 through July 2023.**

147. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

148. Plaintiffs reserve the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

149. Plaintiffs anticipate the issuance of notice setting forth the subject and nature of the instant action to the proposed Class. Upon information and belief, Defendant's own business records or electronic media can be utilized for the notice process.

150. The proposed Class meets the requirements of Federal Rule of Civil Procedure 23.

151. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. Defendant has reported to the Maine Attorney General's Office that the total number of individuals affected in the First Data Breach alone was **13, 231** individuals.[73]

152. **Typicality:** Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through PRGX's uniform misconduct. PRGX's inadequate data security gave rise to Plaintiffs' claims and are identical to those that give rise to the claims of every other Class member because Plaintiffs and each member of the Class had their sensitive PII compromised in the same way by the same conduct of PRGX.

153. **Adequacy:** Plaintiffs are adequate representatives of the Class because Plaintiffs' interests do not conflict with the interests of the Class; Plaintiffs have retained counsel competent and highly experienced in data breach class action litigation; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

---

[73] *See Data Breach Notifications*, OFFICE OF THE MAINE ATTORNEY GENERAL, https://apps.web.maine.gov/online/aeviewer/ME/40/f674c5b1-aad3-4c7f-84ac-422031509727.shtml (last visited Oct. 9, 2023).

154. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress PRGX's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

155. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiffs' and the Class's PII;

c. Whether Defendant owed a duty to Plaintiffs and the Class to adequately protect their PII, and whether it breached this duty;

d. Whether PRGX breached its duties to Plaintiffs and the Class;

e. Whether PRGX failed to provide adequate cyber security;

f. Whether PRGX knew or should have known that its computer and network security systems were vulnerable to cyber attacks;

g. Whether PRGX's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its company network;

h. Whether PRGX was negligent in permitting unencrypted PII off vast numbers of individuals to be stored within its network;

i. Whether PRGX was negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breaches to include former employees and business associates;

j. Whether PRGX breached implied contractual duties to Plaintiffs and the Class to use reasonable care in protecting their PII;

k. Whether PRGX failed to adequately respond to the Data Breaches, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and the Class;

l. Whether PRGX continues to breach duties to Plaintiffs and the Class;

m. Whether Plaintiffs and the Class suffered injury as a proximate result of PRGX's negligent actions or failures to act;

n. Whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief; and

o. Whether PRGX's actions alleged herein constitute gross negligence, and whether Plaintiffs and Class Members are entitled to punitive damages.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

156. Plaintiffs incorporate paragraphs 1–155 as though fully set forth herein.

157. PRGX solicited, gathered, and stored the PII of Plaintiffs and Class Members.

158. Upon accepting and storing the PII of Plaintiffs and Class members on its computer systems and networks, Defendant undertook and owed a duty to Plaintiffs and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiffs and the Class from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

159. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class members could and would suffer if the PII was wrongfully disclosed. Plaintiffs and Class members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class members had no ability to protect their PII that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiffs and the Class.

160. Because of this special relationship, Defendant required Plaintiffs and Class members to provide their PII, including names, Social Security numbers, and other PII.

161. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiffs and Class members in its possession was only used for the provided purpose and that Defendant would destroy any PII that it was not required to maintain.

162. As part of this special relationship, Defendant had a duty to perform with skill, care, and reasonable expedience and faithfulness.

163. Through Defendant's acts and omissions, including Defendant's failure to provide adequate data security, its failure to protect Plaintiffs' and Class members' PII from being foreseeably accessed, and its improper retention of PII it was not required to maintain, Defendant negligently failed to observe and perform its duty.

164. Plaintiffs and Class members did not receive the benefit of the bargain with Defendant, because providing their PII was in exchange for Defendant's implied agreement to secure and keep it safe and to delete it once no longer required.

165. Defendant was aware of the fact that cybercriminals routinely target large corporations through cyberattacks in an attempt to steal customer and employee PII. In other words, Defendant knew of a foreseeable risk to its data security systems but failed to implement reasonable security measures.

166. Defendant owed Plaintiffs and the Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard or delete such data and providing notification to Plaintiffs and the Class members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

167. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

168. Defendant had duties to protect and safeguard the PII of Plaintiffs and the Class from being vulnerable to cyberattacks by taking common-sense

precautions when dealing with sensitive PII. Additional duties that Defendant owed Plaintiffs and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class members' PII was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiffs' and Class members' PII in its possession by using reasonable and adequate security procedures and systems;

c. To implement processes to quickly detect a data breach, security incident, or intrusion involving its networks and servers; and

d. To promptly notify Plaintiffs and Class members of any data breach, security incident, or intrusion that affected or may have affected their PII.

169. Plaintiffs and the Class were the intended beneficiaries of Defendant's duties, creating a special relationship between them and Defendant. Defendant was in a position to ensure that its systems were sufficient to protect the PII that Plaintiffs and the Class had entrusted to it.

170. Plaintiffs' injuries and damages, as described herein, are a reasonably certain consequence of Defendant's negligence and breach of its duties.

171. Defendant breached its duties of care by failing to adequately protect Plaintiffs' and Class members' PII. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, and protecting the PII in its possession;

b. Failing to protect the PII in its possession using reasonable and adequate security procedures and systems;

c. Failing to consistently enforce security policies aimed at protecting Plaintiffs and the Class's PII;

d. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

e. Failing to promptly notify Plaintiffs and Class members of the Data Breaches that affected their PII.

172. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent considering the foreseeable risks and known threats.

173. As a direct and proximate result of Defendant's negligent conduct, including but not limited to its failure to implement and maintain reasonable data security practices and procedures as described above, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

174. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the PII of Plaintiffs and Class members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiffs and Class members while it was within Defendant's possession and control.

175. Further, through its failure to provide timely and clear notification of the Data Breaches to Plaintiffs and Class members, Defendant prevented Plaintiffs and Class members from taking meaningful, proactive steps to securing their PII and mitigating damages.

176. Plaintiffs and Class members could have taken actions earlier had they been timely notified of the Data Breaches.

177. Plaintiffs and Class members could have enrolled in credit monitoring, could have instituted credit freezes, and could have changed their passwords, among other things, had they been alerted to the Data Breaches more quickly.

178. Plaintiffs and Class members have suffered harm from the delay in notifying them of the Data Breaches.

179. As a direct and proximate cause of Defendant's conduct, including but not limited to its failure to implement and maintain reasonable security practices and procedures, Plaintiffs and Class members have suffered, as Plaintiffs have, and/or will suffer injury and damages, including but not limited to: (i) the loss of the

opportunity to determine for themselves how their PII is used; (ii) the publication and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII, including the need for substantial credit monitoring and identity protection services for an extended period of time; (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 Breaches, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports and password protections; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of employees in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives. Thus, Plaintiffs and the Class are entitled to damages in an amount to be proven at trial.

180. The damages Plaintiffs and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's negligent conduct.

181. Plaintiffs and the Class have suffered injury and are entitled to actual and punitive damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class)

182. Plaintiffs incorporate paragraphs 1–155 as though fully set forth herein.

183. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant had a duty to Plaintiffs and the Class to provide fair and adequate computer systems and data security to safeguard the PII of Plaintiffs and the Class.

184. The FTC Act prohibits "unfair practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

185. Defendant gathered and stored the PII of Plaintiffs and the Class as part of their business which affects commerce.

186. Defendant violated the FTC Act by failing to use reasonable measures to protect the PII of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

187. Defendant breached its duties to Plaintiffs and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiffs' and Class members' PII, and by failing to provide prompt notice without reasonable delay.

188. Defendant's multiple failures to comply with applicable laws and regulations constitutes negligence *per se*.

189. Plaintiffs and the Class are within the class of persons that the FTC Act was intended to protect.

190. The harm that occurred as a result of the Data Breaches is the type of harm the FTC Act was intended to guard against.

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

192. Defendant breached its duties to Plaintiffs and the Class by unreasonably delaying and failing to provide notice of the Data Breaches expeditiously and/or as soon as practicable to Plaintiffs and the Class.

193. Defendant's violations of the FTC Act constitute negligence *per se*.

194. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, damages arising from the Data Breaches, as alleged above.

195. The injury and harm that Plaintiffs and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligence *per se*.

196. Plaintiffs and the Class have suffered injury and are entitled to damages in amounts to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

197. Plaintiffs incorporate paragraphs 1–155 as though fully set forth herein.

198. Defendant acquired and maintained the PII of Plaintiffs and the Class including their Social Security numbers and other financial information to provide employment and/or elective benefits.

199. Plaintiffs and Class Members reasonably expected that their PII that they entrusted to PRGX, as part of their employment and/or elective benefits, would remain confidential and would not be shared or disclosed to criminal third parties.

200. Plaintiffs and Defendant had an understanding that Defendant would take steps to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect their sensitive PII and Plaintiffs and Defendant had an expectation that Defendant would not share or disclose, whether intentionally or

unintentionally, sensitive PII in the absence of authorization for any purpose that is not directly related to or beneficial to employment and elective benefits stemming therefrom.

201. Defendant entered into implied contracts with Plaintiffs and the Class in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiffs' and Class Members' PII and timely notify them of a data breach.

202. Based on Defendant's representations, legal obligations, and acceptance of Plaintiffs' and the Class Members' PII, Defendant had an implied duty to safeguard their PII through the use of reasonable industry standards.

203. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' PII and failing to provide them with timely and accurate notice of the Data Breaches. Indeed, it took PRGX over an entire year to warn Plaintiffs and Class Member of the First Data Breach.

204. As a direct and proximate result of Defendant's breach of implied contract, Plaintiffs and the Class Members have suffered damages, including foreseeable consequential damages that Defendant knew about when it requested Plaintiffs' and the Class Members' PII.

205. Plaintiffs and the Class have suffered injuries as described herein, and are entitled to actual and punitive damages, statutory damages, and reasonable attorneys' fees and costs, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

206. Plaintiffs incorporate paragraphs 1–155 as though fully set forth herein.

207. Plaintiffs allege this claim in the alternative to their breach of implied contract claim.

208. Plaintiffs and the Class provided their PII to PRGX to receive employment and/or elective benefits stemming therefrom.

209. By conferring their PII to Defendant, Plaintiffs and the Class reasonably understood Defendant would be responsible for securing their PII in Defendant's possession.

210. Through the collection and use of Plaintiffs' and the Class's PII, Defendant was able to employ Plaintiffs and Class Members. Through employment of Plaintiffs and Class Members, Defendant was able to run its business and receive substantial revenue it otherwise would not have been able to receive.

211. Defendant collected, maintained, and stored the PII of Plaintiffs and the Class, and as such, Defendant had direct knowledge of the monetary benefits conferred upon it by Plaintiff and the Class.

212. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiffs and Class Members and accepted that monetary benefit.

213. However, acceptance of the benefit under the facts and circumstances

outlined above make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breaches, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

214. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures.

215. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

216. If Plaintiffs and Class Members knew that Defendant had not secured their PII, they would not have allowed Defendant to collect their PII.

217. Plaintiffs and Class Members have no adequate remedy at law.

218. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered or will suffer injury, including but not limited to: (i)

actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) 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 Breaches, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession; and/or (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breaches for the remainder of the lives of Plaintiffs and Class Members.

219. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

220. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, all gains that they unjustly received.

FIFTH CAUSE OF ACTION
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and the Class)

221. Plaintiffs incorporate paragraphs 1–155 as though fully set forth herein.

222. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

223. As previously alleged, Plaintiffs and members of the Class are entered into implied contracts with Defendant, which contracts required Defendant to provide adequate security for the PII collected from Plaintiffs and the Class.

224. Defendant owed and still owes a duty of care to Plaintiffs and Class members that require it to adequately secure Plaintiffs' and Class members' PII.

225. Upon reason and belief, Defendant still possesses the PII of Plaintiffs and the Class members.

226. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and the Class members.

227. Since the Data Breaches, Defendant has not yet announced any changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breaches to occur and go undetected and, thereby, prevent further attacks.

228. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and the Class. In fact, now that Defendant's insufficient data security is

known to hackers, the PII in Defendant's possession is even more vulnerable to cyberattack.

229. Actual harm has arisen in the wake of the Data Breaches regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiffs and the members of the Class. Further, Plaintiffs and the members of the Class are at risk of additional or further harm due to the exposure of their PII and Defendant's failure to address the security failings that led to such exposure.

230. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breaches to meet Defendant's contractual obligations and legal duties.

231. Plaintiffs and the Class, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendant engage 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;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment employee data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, customer data not necessary for their provisions of services;

f. Ordering that Defendant conduct regular database scanning and security checks; and

g. Ordering that Defendant routinely and continually conduct 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.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class requested herein;

b. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including compensatory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

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

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

e. A judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

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

VIII. DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all appropriate issues raised in this First Amended Class Action Complaint.

Dated: October 9, 2023

Respectfully submitted,

/s/ William B. Federman
William B. Federman
(*admitted pro hac vice*)
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
T: (405) 235-1560
F: (405) 239-2112
E:wbf@federmanlaw.com

James M. Evangelista
Georgia Bar No. 707807
EVANGELISTA WORLEY LLC
500 Sugar Mill Road Suite 245A
Atlanta, GA 30350
Tel.: 404-205-8400
Fax: 404-205-8395
Email: jim@ewlawllc.com

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the foregoing was electronically filed with the Clerk of Court using the CM/ECF system, which in turn will automatically serve all counsel of record.

Date: October 9, 2023

/s/ William B. Federman

RULE 5.1(C) CERTIFFICATE OF TYPE, FORMAT, AND FONT SIZE

Pursuant to Local Rule 5.1(C) of the United States District Court of the Northern District of Georgia, the undersigned hereby certifies that the foregoing submission to the Court is computer-processed, double spaced between lines, and is typed in Times New Roman font of 14-point size.

/s/ William B. Federman

ClassAction.org
