

Exhibit *A*

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
WEST PALM BEACH DIVISION**

**ANDRE CRAVENS, RYAN GAWRONSKI,
DIANNA J. VIVEROS, GWENDOLYN
KENNEDY, JEREMY ANGELLE and
JOSEPH TYLER HALEY, *on behalf of
themselves and all others similarly situated,***

Plaintiffs,

v.

**GARDA CL SOUTHEAST, INC., GARDA
CL GREAT LAKES, INC., GARDA CL
CENTRAL, INC., GARDA CL
SOUTHWEST, INC., and GARDAWORLD
CASH SERVICES, INC. d/b/a
GARDAWORLD CASH U.S.,**

Defendants.

No. 24-cv-80400

**CONSOLIDATED CLASS ACTION
COMPLAINT**

DEMAND FOR JURY TRIAL

Plaintiffs Andre Cravens, Ryan Gawronski, Dianna J. Viveros, Gwendolyn Kennedy, Jeremy Angelle, and Joseph Tyler Haley (collectively, “Plaintiffs”), through their attorneys, individually and on behalf of all others similarly situated (“Class Members”), bring this Class Action Complaint against Defendants Garda CL Southeast, Inc., Garda CL Great Lakes, Inc., Garda CL Central, Inc., Garda CL Southwest, Inc., and GardaWorld Cash Services, Inc., d/b/a GardaWorld Cash U.S. (collectively, “Garda”), alleging the following on personal knowledge, information and belief, counsel’s investigation, and facts of public record.

NATURE OF ACTION

1. This class action arises from Garda’s failure to protect highly sensitive data entrusted to it by Plaintiffs and Class Members.

2. Garda is “one of the world’s largest privately owned integrated security and risk

company [sic].”¹

3. As such, Garda stores a litany of highly sensitive personal identifiable information (“PII”) and protected health information (“PHI”) belonging to its current and former employees and/or customers. But Garda allowed that PII/PHI to fall into the hands of cybercriminals when criminal hackers infiltrated its insufficiently protected computer systems in a data breach (the “Data Breach”).

4. It is unknown precisely how long the cybercriminals had access to Garda’s network before the Data Breach was discovered. In other words, Garda had no effective means to prevent, detect, stop, or mitigate breaches of its systems, thereby allowing cybercriminals unrestricted access to its current and former employees’ and/or customers’ PII/PHI.

5. On information and belief, cybercriminals were able to breach Garda’s systems because Garda failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect Plaintiffs’ and Class Members’ PII/PHI. In short, Garda’s failures placed Plaintiffs’ and Class Members’ PII/PHI in a vulnerable position, rendering it an easy target for cybercriminals.

6. Plaintiffs are Data Breach victims, having received breach notices from Garda notifying that their sensitive and confidential PII/PHI was accessed in the Data Breach. They bring this class action on behalf of themselves, and all other similarly situated individuals harmed by Garda’s misconduct and the resulting Data Breach.

7. The exposure of one’s PII/PHI to cybercriminals is a bell that cannot be unrung. Before this Data Breach, Garda’s current and former employees’ and/or customers’ private PII/PHI

¹ *Home Page*, GARDA, <https://www.garda.com/> (last visited April 1, 2024).

was exactly that—private. But that is no longer the case. Now, due to the Data Breach, Plaintiffs’ and Class Members’ confidential PII/PHI is forever exposed and insecure.

PARTIES

8. Plaintiff Andre Cravens is a citizen and resident of Mishawaka, Indiana.

9. Plaintiff Ryan Gawronski is a citizen and resident of Cook County, Illinois.

10. Plaintiff Dianna J. Viveros is a citizen and resident of Houston, Texas.

11. Plaintiff Gwendolyn Kennedy is a citizen and resident of Barnhardt, Missouri.

12. Plaintiff Jeremy Angelle is a citizen and resident of Opelousa, Louisiana.

13. Plaintiff Joseph Tyler Haley is a citizen and resident of Hernando, Mississippi.

14. Defendant Garda CL Southeast, Inc. is a profit corporation incorporated in Georgia with its principal place of business at 2000 NW Corporate Boulevard, Boca Raton, Florida, 33431.

15. Defendant Garda CL Great Lakes, Inc., is a profit corporation incorporated in Ohio with its principal place of business at 2000 NW Corporate Boulevard, Boca Raton, Florida, 33431.

16. Defendant Garda CL Central, Inc., is a profit corporation incorporated in Kentucky with its principal place of business at 2000 NW Corporate Boulevard, Boca Raton, Florida, 33431.

17. Defendant Garda CL Southwest, Inc., is a profit corporation incorporated in Texas with its principal place of business at 2000 NW Corporate Boulevard, Boca Raton, Florida, 33431.

18. Defendant GardaWorld Cash Services, Inc. is a general corporation incorporated in Delaware with its principal place of business at 2000 NW Corporate Boulevard, Boca Raton, Florida, 33431.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. Numerous Plaintiffs and Garda are citizens of different states. And there are over 100 putative Class Members.

20. This Court has personal jurisdiction over Garda because it is headquartered in Florida, regularly conducts business in Florida, and has sufficient minimum contacts in Florida.

21. Venue is proper in this Court because Garda's principal office is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

BACKGROUND

Garda Collected and Stored the PII/PHI of Plaintiffs and the Class

22. Garda is "one of the world's largest privately owned integrated security and risk company[ies]."²

23. As part of its business, Garda receives and maintains the PII/PHI of thousands of its current and former employees and/or customers.

24. In collecting and maintaining employees' and customers' PII/PHI, Garda agreed to safeguard that sensitive data in accordance with its internal policies, state law, and federal law. After all, Plaintiffs and Class Members themselves took reasonable steps to secure their PII/PHI and reasonably expected the same level of care from Garda, a sophisticated business entity.

² Home Page, GARDA, <https://www.garda.com/> (last visited April 1, 2024).

25. Under state and federal law, businesses like Garda have duties to protect current and former employees' and/or customers' PII/PHI and timely and adequately notify them about data breaches compromising that information.

26. Garda recognizes these duties, declaring the following in the "Privacy Notice" posted on Garda's website³:

- a. "At GardaWorld, we understand the importance of privacy and are committed to protecting your personal data."
- b. "We only use your personal data where permitted by applicable law."
- c. "We will obtain your express consent before sharing your personal data[.]"
- d. "We require all third parties to respect the security of your personal data and to treat it in accordance with applicable law."
- e. "We ensure that your personal data is protected by requiring all our group companies to follow the same rules when processing your personal data."
- f. "We have implemented appropriate security measures to prevent your personal data from being accidentally lost or used, accessed, modified or communicated in an unauthorized manner."
- g. "In addition, we restrict access to your personal data to employees, agents, contractors and other third parties who need to know it for business purposes. They will only process your personal data in accordance with our instructions and are subject to an obligation of confidentiality."
- h. "We have procedures in place to deal with any suspected personal data breach[.]"
- i. "GardaWorld is committed to protecting your personal information throughout its life cycle in accordance with its privacy practices and in compliance with the requirements of applicable laws."

³ *Privacy Notice*, GARDA, <https://www.garda.com/privacy-notice> (last visited April 1, 2024).

- j. “GardaWorld has adopted an internal data governance policy that sets out the principles governing the protection of personal data in the context of its operations.”
- k. “GardaWorld recognizes the importance of the protection, confidentiality and security of the personal data it processes in the course of its activities, and of making its employees and partners aware of this.”
- l. “[W]e do not share your personal information with third parties without your consent, except where permitted by law.”
- m. “GardaWorld must take reasonable steps to reduce the risk of serious harm and review its practices to prevent similar privacy incidents in the future.”

Garda’s Data Breach

27. From October 30, 2023, until November 16, 2023, Garda’s network was hacked in the Data Breach when “an unauthorized actor accessed some of [its] facility systems in Florida” and then “copied [files] from those systems.”⁴

28. Worryingly, Garda failed to detect the Data Breach until November 16, 2023. Thus, cybercriminals had a *full 17 days* to peruse and exfiltrate PII/PHI before being detected.

29. Because of Garda’s Data Breach, at least the following types of PII/PHI were compromised⁵:

- a. names;
- b. addresses;
- c. Social Security numbers;

⁴ *Data Breach Notifications*, MAINE ATTY GEN, <https://apps.web.maine.gov/online/aewiewer/ME/40/b259cad1-d4ba-46cf-9a2a-05ff391ebfcc.shtml> (last visited April 1, 2024).

⁵ *Id.*; *Data Security Breach Reports*, ATTY GEN TEXAS, <https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage> (last visited April 1, 2024).

- d. driver's license numbers;
- e. dates of birth;
- f. health insurance information;
- g. health benefit information;
- h. medical information.

30. In total, Garda injured at least 39,928 persons via the exposure of their PII/PHI in the Data Breach.⁶ Upon information and belief, these 39,928 persons include its current and former employees and/or customers.

31. Yet, Garda waited over until March 22, 2024—a full 127 days after it discovered its Data Breach—before notifying Plaintiffs and Class Members their PII/PHI was compromised.⁷

32. Thus, Garda kept Plaintiffs and Class Members in the dark, thereby depriving them of the opportunity to mitigate their injuries resulting from the Data Breach in a timely manner.

33. When Garda did send Plaintiffs and Class Members its Notice of Data Breach letter alerting them about the Data Breach, it acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiffs and Class Members⁸:

- a. “We also encourage you to remain vigilant against incidents of identity theft and fraud by engaging in the following best practices . . . [c]hange your passwords regularly and make sure they are secure.”
- b. “[B]e vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity.”

⁶ *Data Breach Notifications*, MAINE ATTY GEN, <https://apps.web.maine.gov/online/aeviewer/ME/40/b259cad1-d4ba-46cf-9a2a-05ff391ebfcc.shtml> (last visited April 1, 2024).

⁷ *Id.*

⁸ *Id.*

- c. “[C]ontact the Federal Trade Commission and/or the Attorney General’s office in your home state . . . for information on how to prevent or avoid identity theft.”

34. Garda breached its duties to take reasonable steps to protect Plaintiffs’ and Class Members’ sensitive and confidential PII/PHI by using inadequate security practices, which ultimately caused the Data Breach. In other words, Garda’s negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing Plaintiffs’ and Class Members’ PII/PHI. Through this failure and the resulting Data Breach, Garda caused widespread injury and monetary damages.

35. Since the Data Breach, Garda has declared that it “took additional steps to secure [its] systems.”⁹ But this is too little too late. Simply put, these measures, which Garda now recognizes as necessary, should have been implemented *before* the Data Breach.

36. On information and belief, Garda failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

37. Further, Garda’s Notice of Data Breach shows that Garda cannot, or will not, determine the full scope of the Data Breach, as Garda has been unable to determine precisely what information was stolen and when.

38. Garda has done little to remedy its Data Breach. While Garda has offered some Data Breach victims credit monitoring and identity-related services, such services are wholly insufficient to compensate Plaintiffs and Class members for the injuries that Garda inflicted upon them in causing the Data Breach. Moreover, some Plaintiffs attempted to obtain the services Garda offered but were unable to do so despite following the Notice of Data Breach’s instructions.

⁹ *Id.*

39. Because of Garda's Data Breach, Plaintiffs' and Class Members' sensitive PII/PHI was placed into the hands of cybercriminals, inflicting numerous injuries and significant damages upon Plaintiffs and Class members.

Metaencryptor & the Dark Web

40. Worryingly, the hackers that obtained Plaintiffs' and Class members' PII/PHI are part of the notorious cybercriminal group "Metaencryptor."¹⁰

41. The cyber security company "Hackmanac" reported that Metaencryptor exfiltrated 300 gigabytes of data, and then threatened to *publish* the data unless a ransom was paid by December 22, 2023.¹¹

¹⁰ *Hacks of Today*, HACKMANAC, (Dec. 7, 2023) <https://hackmanac.com/news/hacks-of-today-07-12-2023>.

¹¹ *Id.*

GARDAWORLD

Victim website:	garda.com
Victim country:	Canada
Attacker name:	Metaencryptor
Attacker class:	Cybercrime
Attack technique:	Ransomware
Ransom demand:	N/A
Exfiltrated data amount:	300 GB
Exfiltrated data type:	N/A
Leaked data:	/
Ransom deadline:	22 nd Dec 23
Cyber Risk Factor:	4

42. Likewise, several other cyber security companies have confirmed Metaencryptor's involvement in the Data Breach.¹²

Group	Title	Date
Metaencryptor	Garda	2023-12-07
Garda		

¹² Metaencryptor, RANSOMLOOK, <https://www.ransomlook.io/group/metaencryptor> (last visited April 1, 2024); Garda, BREACHSENSE, <https://www.breachsense.com/breaches/garda-data-breach/> (last visited April 1, 2024); ThreatMon Advanced Ransomware Monitoring (@TMRansomMonitor), TWITTER (Dec. 7, 2023) <https://twitter.com/TMRansomMonitor/status/1732771508731142588>.

Data Breach Report	
Victim	garda.com
Threat Actor	Metaencryptor
Date Discovered	Dec 08, 2023
Description	Garda World Security Corporation provides security solutions, cash logistics, and risk consulting services.
Leak Size	Unknown

 **Post**

 **ThreatMon Advanced Ransomware Monitoring** 
@TMRansomMonitor

Actor : metaencryptor
Victim : Garda
Date : 2023-12-07 17:34 UTC +3

According to [#DarkWeb](#) [#Ransomware](#) activity detected by the ThreatMon Threat Intelligence Team. The “[#metaencryptor](#)” Ransomware group has added Garda to its victims.

8:38 AM · Dec 7, 2023 · **523** Views

43. Worryingly, Metaencryptor is notorious for ***publishing*** stolen data on the Dark Web.¹³ For example, a third-party report explained that Metaencryptor “is a new ransomware gang that published the data of 12 victims in August 2023.”¹⁴

44. And screenshots of Metaencryptor’s Dark Web website confirm that stolen PII/PHI was published for ***at least*** the following data breaches:

- a. Vega Reederei GmbH & Co. KG;¹⁵
- b. Dillon Supply;¹⁶
- c. Epicure;¹⁷
- d. Coswell;¹⁸
- e. BOB Automotive Group;¹⁹
- f. Seoul Semiconductor;²⁰

¹³ *Ransomware review: September 2023*, MALWAREBYTES (Sept. 12, 2023) <https://www.malwarebytes.com/blog/threat-intelligence/2023/09/ransomware-review-september-2023>.

¹⁴ *Id.*

¹⁵ *Vega Reederei GmbH & Co. KG*, RANSOMLOOK, <https://www.ransomlook.io/screenshots/metaencryptor/Vega%20Reederei%20GmbH%20%26%20Co%20KG.png> (last visited May 14, 2024).

¹⁶ *Dillon Supply*, RANSOMLOOK, <https://www.ransomlook.io/screenshots/metaencryptor/Dillon%20Supply.png> (last visited May 14, 2024).

¹⁷ *Epicure*, RANSOMLOOK, <https://www.ransomlook.io/screenshots/metaencryptor/Epicure.png> (last visited May 14, 2024).

¹⁸ *Coswell*, RANSOMLOOK, <https://www.ransomlook.io/screenshots/metaencryptor/Coswell.png> (last visited May 14, 2024).

¹⁹ *BOB Automotive Group*, RANSOMLOOK, <https://www.ransomlook.io/screenshots/metaencryptor/BOB%20Automotive%20Group.png> (last visited May 14, 2024).

²⁰ *Seoul Semiconductor*, RANSOMLOOK, <https://www.ransomlook.io/screenshots/metaencryptor/Seoul%20Semiconductor.png> (last visited May 14, 2024).

- g. Autohaus Ebert GmbH;²¹
- h. CVO Antwerpen;²²
- i. ICON Creative Studio;²³
- j. Heilmann Gruppe;²⁴
- k. Schwälbchen Molkerei AG;²⁵ and
- l. Münchner Verlag Gruppe GmbH.²⁶

45. For example, below is a screenshot of Metaencryptor's Dark Web page for the "Vega Reederei GmbH & Co. KG" data breach. It reveals that Metaencryptor published the "FULL" set of stolen information on May 7, 2024.²⁷

²¹ *Autohaus Ebert GmbH*, RANSOMLOOK, <https://www.ransomlook.io/screenshots/metaencryptor/Autohaus%20Ebert%20GmbH.png> (last visited May 14, 2024).

²² *CVO Antwerpen*, RANSOMLOOK, <https://www.ransomlook.io/screenshots/metaencryptor/CVO%20Antwerpen.png> (last visited May 14, 2024).

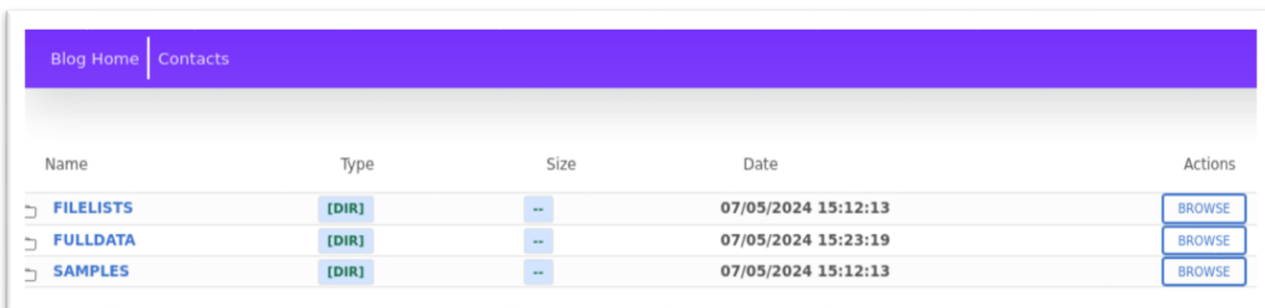
²³ *ICON Creative Studio*, RANSOMLOOK, <https://www.ransomlook.io/screenshots/metaencryptor/ICON%20Creative%20Studio.png> (last visited May 14, 2024).

²⁴ *Heilmann Gruppe*, RANSOMLOOK, <https://www.ransomlook.io/screenshots/metaencryptor/Heilmann%20Gruppe.png> (last visited May 14, 2024).

²⁵ *Schwälbchen Molkerei AG*, RANSOMLOOK, <https://www.ransomlook.io/screenshots/metaencryptor/Schw%C3%A4lbchen%20Molkerei%20AG.png> (last visited May 14, 2024).

²⁶ *Münchner Verlagsgruppe GmbH*, RANSOMLOOK, <https://www.ransomlook.io/screenshots/metaencryptor/M%C3%BCnchner%20Verlagsgruppe%20GmbH.png> (last visited May 14, 2024).

²⁷ *Vega Reederei GmbH & Co. KG*, RANSOMLOOK, <https://www.ransomlook.io/screenshots/metaencryptor/Vega%20Reederei%20GmbH%20%26%20Co%20KG.png> (last visited May 14, 2024).



Name	Type	Size	Date	Actions
FILELISTS	[DIR]	--	07/05/2024 15:12:13	BROWSE
FULLDATA	[DIR]	--	07/05/2024 15:23:19	BROWSE
SAMPLES	[DIR]	--	07/05/2024 15:12:13	BROWSE

46. Likewise, for the “BOB Automotive Group” data breach, Metaencrytor published the following types of stolen information (here, the names of individuals are redacted to preserve their privacy).²⁸

²⁸ BOB Automotive Group, RANSOMLOOK, <https://www.ransomlook.io/screenshots/metaencrytor/BOB%20Automotive%20Group.png> (last visited May 14, 2024).

Blog Home Contacts				
Name	Type	Size	Date	Actions
 Appl	[DIR]	--	10/08/2023 16:12:36	BROWSE
 BOB-Dateiserver	[DIR]	--	10/08/2023 16:12:36	BROWSE
 	[DIR]	--	10/08/2023 16:12:36	BROWSE
 Personal	[DIR]	--	10/08/2023 16:12:39	BROWSE
 	[DIR]	--	10/08/2023 16:12:35	BROWSE
 	[DIR]	--	10/08/2023 16:12:34	BROWSE
 dat	[DIR]	--	10/08/2023 16:06:11	BROWSE
 filelists	[DIR]	--	10/08/2023 16:19:17	BROWSE
 fulldump	[DIR]	--	10/08/2023 16:19:17	BROWSE
 samples	[DIR]	--	10/08/2023 16:19:17	BROWSE
 	[DIR]	--	10/08/2023 16:12:36	BROWSE
 datfin2.part01.rar	[FIL]	500 MB	10/08/2023 16:16:34	DOWNLOAD
 datfin2.part02.rar	[FIL]	500 MB	10/08/2023 16:16:39	DOWNLOAD
 datfin2.part03.rar	[FIL]	500 MB	10/08/2023 16:16:44	DOWNLOAD
 datfin2.part04.rar	[FIL]	500 MB	10/08/2023 16:16:50	DOWNLOAD
 datfin2.part05.rar	[FIL]	500 MB	10/08/2023 16:16:55	DOWNLOAD
 datfin2.part06.rar	[FIL]	500 MB	10/08/2023 16:17:03	DOWNLOAD
 datfin2.part07.rar	[FIL]	500 MB	10/08/2023 16:17:10	DOWNLOAD
 datfin2.part08.rar	[FIL]	500 MB	10/08/2023 16:17:13	DOWNLOAD
 datfin2.part09.rar	[FIL]	500 MB	10/08/2023 16:17:20	DOWNLOAD
 datfin2.part10.rar	[FIL]	500 MB	10/08/2023 16:17:27	DOWNLOAD
 datfin2.part11.rar	[FIL]	500 MB	10/08/2023 16:17:31	DOWNLOAD
 datfin2.part12.rar	[FIL]	500 MB	10/08/2023 16:17:38	DOWNLOAD
 datfin2.part13.rar	[FIL]	500 MB	10/08/2023 16:17:43	DOWNLOAD
 datfin2.part14.rar	[FIL]	500 MB	10/08/2023 16:17:49	DOWNLOAD
 datfin2.part15.rar	[FIL]	500 MB	10/08/2023 16:17:56	DOWNLOAD
 datfin2.part16.rar	[FIL]	500 MB	10/08/2023 16:18:01	DOWNLOAD
 datfin2.part17.rar	[FIL]	500 MB	10/08/2023 16:18:06	DOWNLOAD
 datfin2.part18.rar	[FIL]	500 MB	10/08/2023 16:18:14	DOWNLOAD
 datfin2.part19.rar	[FIL]	500 MB	10/08/2023 16:18:17	DOWNLOAD
 datfin2.part20.rar	[FIL]	500 MB	10/08/2023 16:18:22	DOWNLOAD
 datfin2.part21.rar	[FIL]	500 MB	10/08/2023 16:18:31	DOWNLOAD
 datfin2.part22.rar	[FIL]	500 MB	10/08/2023 16:18:36	DOWNLOAD
 datfin2.part23.rar	[FIL]	500 MB	10/08/2023 16:18:44	DOWNLOAD
 datfin2.part24.rar	[FIL]	500 MB	10/08/2023 16:18:49	DOWNLOAD
 datfin2.part25.rar	[FIL]	500 MB	10/08/2023 16:18:55	DOWNLOAD
 datfin2.part26.rar	[FIL]	500 MB	10/08/2023 16:19:01	DOWNLOAD
 datfin2.part27.rar	[FIL]	500 MB	10/08/2023 16:19:07	DOWNLOAD
 datfin2.part28.rar	[FIL]	317.82 MB	10/08/2023 16:19:15	DOWNLOAD
 filaksp.part01.rar	[FIL]	1000 MB	10/08/2023 16:12:47	DOWNLOAD
 filaksp.part02.rar	[FIL]	547.17 MB	10/08/2023 16:12:59	DOWNLOAD
 irwdb.part01.rar	[FIL]	1000 MB	10/08/2023 16:13:04	DOWNLOAD
 irwdb.part02.rar	[FIL]	1000 MB	10/08/2023 16:13:16	DOWNLOAD
 irwdb.part03.rar	[FIL]	1000 MB	10/08/2023 16:13:28	DOWNLOAD
 irwdb.part04.rar	[FIL]	1000 MB	10/08/2023 16:13:38	DOWNLOAD
 irwdb.part05.rar	[FIL]	1000 MB	10/08/2023 16:13:49	DOWNLOAD
 irwdb.part06.rar	[FIL]	1000 MB	10/08/2023 16:14:03	DOWNLOAD
 irwdb.part07.rar	[FIL]	1000 MB	10/08/2023 16:14:14	DOWNLOAD
 irwdb.part08.rar	[FIL]	1000 MB	10/08/2023 16:14:26	DOWNLOAD
 irwdb.part09.rar	[FIL]	1000 MB	10/08/2023 16:14:36	DOWNLOAD
 irwdb.part10.rar	[FIL]	1000 MB	10/08/2023 16:14:49	DOWNLOAD
 irwdb.part11.rar	[FIL]	1000 MB	10/08/2023 16:15:01	DOWNLOAD
 irwdb.part12.rar	[FIL]	1000 MB	10/08/2023 16:15:12	DOWNLOAD
 irwdb.part13.rar	[FIL]	1000 MB	10/08/2023 16:15:26	DOWNLOAD
 irwdb.part14.rar	[FIL]	1000 MB	10/08/2023 16:15:37	DOWNLOAD
 irwdb.part15.rar	[FIL]	1000 MB	10/08/2023 16:15:48	DOWNLOAD
 irwdb.part16.rar	[FIL]	1000 MB	10/08/2023 16:16:01	DOWNLOAD
 irwdb.part17.rar	[FIL]	1000 MB	10/08/2023 16:16:13	DOWNLOAD
 irwdb.part18.rar	[FIL]	642.19 MB	10/08/2023 16:16:25	DOWNLOAD
 sampledb.rar	[FIL]	2.21 MB	10/08/2023 16:12:34	DOWNLOAD

47. Thus, upon information and belief, Plaintiffs' and Class Members' stolen PII/PHI has already been published, or will be published imminently, by Metaencryptor on the Dark Web.

Plaintiff Andre Cravens's Experiences and Injuries

48. Plaintiff Andre Cravens is a former employee of Garda, having worked for Garda from approximately 2019 until 2021.

49. Thus, Garda obtained and maintained Plaintiff Cravens's PII/PHI.

50. As a result, Plaintiff Cravens was injured by Garda's Data Breach.

51. As a condition of his employment with Defendant, Plaintiff Cravens provided Garda with his PII/PHI. Garda required Plaintiff Cravens to provide his PII/PHI in order to obtain employment and payment for that employment, and used that PII/PHI to facilitate its employment of Plaintiff Cravens, including payroll.

52. Plaintiff Cravens provided his PII/PHI to Garda and trusted the company would use reasonable measures to protect it according to Garda's internal policies, as well as state and federal law. Garda obtained and continues to maintain Plaintiff Craven's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

53. Plaintiff Cravens reasonably understood that a portion of the funds derived from his employment would be used to pay for adequate cybersecurity and protection of PII/PHI.

54. Plaintiff Cravens does not recall ever learning that his information was compromised in a data breach incident, other than the Data Breach at issue here.

55. Plaintiff Cravens received a Notice of Data Breach on March 28, 2024.

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

57. Through its Data Breach, Garda compromised Plaintiff Cravens's name, Social

Security number, driver's license number, date of birth, insurance information, benefit information, and health information.

58. Plaintiff Cravens has spent, and will continue to spend, significant time and effort monitoring his accounts to protect himself from identity theft. After all, Garda directed Plaintiff Cravens to take those steps in its Notice of Data Breach. In particular, Plaintiff Cravens contacted the banks with which he has client relationships, paused credit cards temporarily, placed restrictions on certain financial accounts, and signed up for credit monitoring, and continues to review bank and credit card statements carefully each month.

59. Following the Data Breach, Plaintiff Cravens was notified that an unknown actor submitted an insurance inquiry in Plaintiff Cravens' name without his authorization.

60. In addition, Plaintiff Cravens has suffered from a spike in spam and scam phone calls in the aftermath of the Data Breach.

61. Plaintiff Cravens fears for his personal financial security and worries about what information was exposed in the Data Breach.

62. Because of Garda's Data Breach, Plaintiff Cravens has suffered, and will continue to suffer, anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Cravens's injuries are precisely the type of injuries that the law contemplates and addresses.

63. Plaintiff Cravens suffered actual injury from the exposure and theft of his PII/PHI, which exposure violates his rights to privacy.

64. Plaintiff Cravens suffered actual injury by being deprived of the benefit of the bargain (vis-à-vis his employment with Garda).

65. Plaintiff Cravens suffered actual injury in the form of damages to and diminution

in the value of his PII/PHI. After all, PII/PHI is a form of intangible property—property that Garda was required to adequately protect.

66. Plaintiff Cravens suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Garda’s Data Breach placed Plaintiff Cravens’s PII/PHI right in the hands of criminals.

67. Because of the Data Breach, Plaintiff Cravens has spent, and anticipates spending in the future, considerable amounts of time and money to try and mitigate his injuries.

68. Following the Data Breach, Plaintiff Cravens enrolled in a credit monitoring service for which he has incurred, and will continue to incur, monthly costs that he would not have to pay but for Garda’s Data Breach.

69. Today, Plaintiff Cravens has a continuing interest in ensuring that his PII/PHI—which, upon information and belief, remains backed up in Garda’s possession—is protected and safeguarded from additional breaches.

Plaintiff Ryan Gawronski’s Experiences and Injuries

70. Plaintiff Gawronski is a former employee of Garda, having worked for Garda from approximately 2016 to 2019.

71. Thus, Garda obtained and maintained Plaintiff Gawronski’s PII/PHI.

72. As a result, Plaintiff Gawronski was injured by Garda’s Data Breach.

73. As a condition of his employment with Defendant, Plaintiff Gawronski provided Garda with his PII/PHI. Garda required Plaintiff Gawronski to provide his PII/PHI in order to obtain employment and payment for that employment, and used that PII/PHI to facilitate its employment of Plaintiff, including payroll.

74. Plaintiff Gawronski provided his PII/PHI to Garda and trusted the company would

use reasonable measures to protect it according to Garda's internal policies, as well as state and federal law. Garda obtained and continues to maintain Plaintiff Gawronski's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

75. Plaintiff Gawronski reasonably understood that a portion of the funds derived from his employment would be used to pay for adequate cybersecurity and protection of PII/PHI.

76. Plaintiff Gawronski does not recall ever learning that his information was compromised in a data breach incident, other than the Data Breach at issue here.

77. Plaintiff Gawronski received a Notice of Data Breach dated March 22, 2024.

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

79. Through its Data Breach, Garda compromised Plaintiff Gawronski's name, Social Security number, date of birth, driver's license number, and insurance, benefit, or other health-related information.

80. Plaintiff Gawronski has spent, and will continue to spend, significant time and effort monitoring his accounts to protect himself from identity theft. After all, Garda directed Plaintiff Gawronski to take those steps in its Notice of Data Breach.

81. In particular, Plaintiff Gawronski spent time researching and verifying the legitimacy of the Data Breach, researching the credit monitoring and identity theft protection services offered by Defendant, changing passwords, and resecuring his own computer network.

82. In the aftermath of the Data Breach, Plaintiff Gawronski has suffered from a spike in spam and scam phone calls and texts.

83. Plaintiff Gawronski fears for his personal financial security and worries about what

information was exposed in the Data Breach.

84. Because of Garda's Data Breach, Plaintiff Gawronski has suffered, and will continue to suffer, anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Gawronski's injuries are precisely the type of injuries that the law contemplates and addresses.

85. Plaintiff Gawronski suffered actual injury from the exposure and theft of his PII/PHI, which violates his rights to privacy.

86. Plaintiff Gawronski suffered actual injury by being deprived of the benefit of the bargain (vis-à-vis his employment with Garda).

87. Plaintiff Gawronski suffered actual injury in the form of damages to and diminution in the value of his PII/PHI. After all, PII/PHI is a form of intangible property—property that Garda was required to adequately protect.

88. Plaintiff Gawronski suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Garda's Data Breach placed Plaintiff Gawronski's PII/PHI right in the hands of criminals.

89. Because of the Data Breach, Plaintiff Gawronski has spent, and anticipates spending in the future, considerable amounts of time and money to try and mitigate his injuries.

90. Today, Plaintiff Gawronski has a continuing interest in ensuring that his PII/PHI—which, upon information and belief, remains backed up in Garda's possession—is protected and safeguarded from additional breaches.

Plaintiff Dianna Viveros's Experiences and Injuries

91. Plaintiff Viveros is a former employee of Garda, having worked for Garda from approximately 2018 to 2021.

92. Thus, Garda obtained and maintained Plaintiff Viveros's PII/PHI.

93. As a result, Plaintiff Viveros was injured by Garda's Data Breach.

94. As a condition of her employment with Defendant, Plaintiff Viveros provided Garda with her PII/PHI. Garda required Plaintiff Viveros to provide her PII/PHI in order to obtain employment and payment for that employment, and used that PII/PHI to facilitate its employment of Plaintiff Viveros, including payroll.

95. Plaintiff Viveros provided her PII/PHI to Garda and trusted the company would use reasonable measures to protect it according to Garda's internal policies, as well as state and federal law. Garda obtained and continues to maintain Plaintiff Viveros's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

96. Plaintiff Viveros reasonably understood that a portion of the funds derived from her employment would be used to pay for adequate cybersecurity and protection of PII/PHI.

97. Plaintiff Viveros does not recall ever learning that her information was compromised in a data breach incident, other than the Data Breach at issue here.

98. Plaintiff Viveros received a Notice of Data Breach dated March 22, 2024.

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

100. Through its Data Breach, Garda compromised Plaintiff Viveros's PII/PHI, which upon information and belief includes her name, Social Security number, driver's license number, date of birth, and/or insurance, benefit, or other health-related information.

101. Plaintiff Viveros has spent, and will continue to spend, significant time and effort monitoring her accounts to protect herself from identity theft. After all, Garda directed Plaintiff Viveros to take those steps in its Notice of Data Breach.

102. In the aftermath of the Data Breach, Plaintiff Viveros has suffered from a spike in spam and scam text messages.

103. To make matters worse, Plaintiff was notified by the cybersecurity service “Keeper” that her personal information was found ***published*** on the Dark Web.

104. In fact, Plaintiff Viveros *already* suffered from substantial identity theft and fraud.

105. On February 24, 2024, Plaintiff Viveros received a notification from her bank that a suspicious charge was charged to her Capital One account. Thereafter, Plaintiff Viveros confirmed that she did not make the purchase and Capital One determined the transaction was fraudulent.

106. Later, on April 2, 2024, Plaintiff Viveros received a notification from her Navy Federal Credit Union that a fraudulent charge was made on her account in France. But Plaintiff Viveros never made any such purchase in France using her Navy Federal Credit Union debit card. As such, the bank determined that the transaction was fraudulent.

107. As a result of the multiple fraudulent transactions, Plaintiff Viveros was forced to close both existing accounts and open new accounts with Navy Federal Credit Union and Capital One. During this period of disruption, Plaintiff was deprived of the ability to readily access her funds.

108. Thereafter, Plaintiff Viveros spent significant time attempting to mitigate the fallout of the Data Breach. In particular, she has already spent approximately 50 hours, *inter alia*, cancelling her debit card accounts, researching and verifying the legitimacy of the Data Breach, opening new debit accounts, putting locks on her debit and credit cards, searching for identity theft protection services, resolving issues related to fraudulent charges, and traveling to her Navy Federal branch to get a new debit card.

109. Additionally, Plaintiff Viveros incurred a fee of \$150.00 when an automatic charge failed due to the compromise of her Navy Federal debit account.

110. Moreover, Plaintiff received numerous emails notifying that loans were approved in her name. But critically, Plaintiff Viveros never applied for these loans. This further underscores the fact that Plaintiff Viveros has become a target of substantial identity theft and fraud following the Data Breach.

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

112. Because of Garda's Data Breach, Plaintiff Viveros has suffered, and will continue to suffer, anxiety, sleep disruption, stress, fear, and frustration, including fear of identity theft, negative impacts on her credit, and accounts being fraudulently opened in her name, which fears have already manifested. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Viveros's injuries are precisely the type of injuries that the law contemplates and addresses.

113. Plaintiff Viveros suffered actual injury from the exposure and theft of her PII/PHI, which violates her rights to privacy.

114. Plaintiff Viveros suffered actual injury by being deprived of the benefit of the bargain (vis-à-vis her employment with Garda).

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

116. Plaintiff Viveros suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Garda's Data Breach

placed Plaintiff Viveros's PII/PHI right in the hands of criminals.

117. Because of the Data Breach, Plaintiff Viveros has spent, and anticipates spending in the future, considerable amounts of time and money to try and mitigate her injuries.

118. Today, Plaintiff Viveros has a continuing interest in ensuring that her PII/PHI—which, upon information and belief, remains backed up in Garda's possession—is protected and safeguarded from additional breaches.

Plaintiff Gwendolyn Kennedy's Experiences and Injuries

119. Plaintiff Kennedy is a former employee of Garda, having worked for Garda from approximately 2016 until 2017.

120. Thus, Garda obtained and maintained Plaintiff Kennedy's PII/PHI.

121. As a result, Plaintiff Kennedy was injured by Garda's Data Breach.

122. As a condition of her employment with Garda, Plaintiff Kennedy provided Garda with her PII/PHI. Garda required Plaintiff Kennedy to provide her PII/PHI in order to obtain employment and payment for that employment, and used that PII/PHI to facilitate its employment of Plaintiff Kennedy, including payroll.

123. Plaintiff Kennedy provided her PII/PHI to Garda and trusted the company would use reasonable measures to protect it according to Garda's internal policies, as well as state and federal law. Garda obtained and continues to maintain Plaintiff's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

124. Plaintiff Kennedy reasonably understood that a portion of the funds derived from her employment would be used to pay for adequate cybersecurity and protection of PII/PHI.

125. Plaintiff Kennedy does not recall ever learning that her information was compromised in a data breach incident, other than the Data Breach at issue here.

126. Plaintiff Kennedy received a Notice of Data Breach from Garda dated March 22, 2024.

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

128. Through its Data Breach, Garda compromised Plaintiff Kennedy's PII/PHI, which upon information and belief includes her name, Social Security number, driver's license number, date of birth, and/or insurance, benefit, or other health-related information.

129. Plaintiff Kennedy has spent, and will continue to spend, significant time and effort monitoring her accounts to protect herself from identity theft. After all, Garda directed Plaintiff Kennedy to take those steps in its Notice of Data Breach.

130. In particular, Plaintiff Kennedy spent hours responding to the fallout of the Data Breach, time which she would have dedicated to other endeavors but for the Data Breach. For example, she spent time signing up for credit monitoring, carefully reviewing her accounts, calling and talking with a representative from CyEx, and requesting her credit reports.

131. In the aftermath of the Data Breach, Plaintiff Kennedy has suffered from a spike in spam and scam phone calls.

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

133. Because of Garda's Data Breach, Plaintiff Kennedy has suffered, and will continue to suffer, anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Kennedy's injuries are precisely the type of injuries that the law contemplates and addresses.

134. Plaintiff Kennedy suffered actual injury from the exposure and theft of her PII/PHI,

which violates her rights to privacy.

135. Plaintiff Kennedy suffered actual injury by being deprived of the benefit of the bargain (vis-à-vis her employment with Garda).

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

137. Plaintiff Kennedy suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Garda’s Data Breach placed Plaintiff Kennedy’s PII/PHI right in the hands of criminals.

138. Because of the Data Breach, Plaintiff Kennedy has spent, and anticipates spending in the future, considerable amounts of time and money to try and mitigate her injuries.

139. Today, Plaintiff Kennedy has a continuing interest in ensuring that her PII/PHI—which, upon information and belief, remains backed up in Garda’s possession—is protected and safeguarded from additional breaches.

Plaintiff Jeremy Angelle’s Experiences and Injuries

140. Plaintiff Angelle is a former employee of Garda, having worked for Garda from approximately 2014 until 2021.

141. Thus, Garda obtained and maintained Plaintiff Angelle’s PII/PHI.

142. As a result, Plaintiff Angelle was injured by Garda’s Data Breach.

143. As a condition of his employment with Defendant, Plaintiff Angelle provided Garda with his PII/PHI. Garda required Plaintiff Angelle to provide his PII/PHI in order to obtain employment and payment for that employment, and used that PII/PHI to facilitate its employment of Plaintiff Angelle, including payroll.

144. Plaintiff Angelle provided his PII/PHI to Garda and trusted the company would use reasonable measures to protect it according to Garda's internal policies, as well as state and federal law. Garda obtained and continues to maintain Plaintiff Angelle's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

145. Plaintiff Angelle reasonably understood that a portion of the funds derived from his employment would be used to pay for adequate cybersecurity and protection of PII/PHI.

146. Plaintiff Angelle received a Notice of Data Breach from Garda dated March 22, 2024.

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

148. Through its Data Breach, Garda compromised Plaintiff Angelle's PII/PHI including his name, Social Security number, driver's license number, date of birth, and/or insurance, benefit, or other health-related information.

149. Plaintiff Angelle has spent, and will continue to spend, significant time and effort monitoring his accounts to protect himself from identity theft. After all, Garda directed Plaintiff Angelle to take those steps in its Notice of Data Breach. For example, Plaintiff has spent time changing passwords, contacting his bank, and continually monitoring his financial accounts.

150. Plaintiff Angelle fears for his personal financial security and worries about what information was exposed in the Data Breach.

151. Because of Garda's Data Breach, Plaintiff Angelle has suffered, and will continue to suffer, anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Angelle's injuries are precisely the type of injuries that the law contemplates and addresses.

152. In the aftermath of the Data Breach, Plaintiff Angelle has suffered from a spike in spam and scam phone calls, text messages, and emails. Because Plaintiff Angelle works at night and sleeps during the day, these spam communications often interrupt his sleep and have caused significant disruptions to Plaintiff Angelle's daily life.

153. Plaintiff Angelle suffered actual injury from the exposure and theft of his PII/PHI, which violates his rights to privacy.

154. Plaintiff Angelle suffered actual injury by being deprived of the benefit of the bargain (vis-à-vis his employment with Garda).

155. Plaintiff Angelle suffered actual injury in the form of damages to and diminution in the value of his PII/PHI. After all, PII/PHI is a form of intangible property—property that Garda was required to adequately protect.

156. Plaintiff Angelle suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Garda's Data Breach placed Plaintiff Angelle's PII/PHI right in the hands of criminals.

157. Because of the Data Breach, Plaintiff Angelle has spent, and anticipates spending in the future, considerable amounts of time and money to try and mitigate his injuries.

158. Today, Plaintiff Angelle has a continuing interest in ensuring that his PII/PHI—which, upon information and belief, remains backed up in Garda's possession—is protected and safeguarded from additional breaches.

Plaintiff Joseph Haley's Experiences and Injuries

159. Plaintiff Haley is a former employee of Garda, having worked for Garda from approximately 2022 until 2023.

160. Thus, Garda obtained and maintained Plaintiff Haley's PII/PHI.

161. As a result, Plaintiff Haley was injured by Garda's Data Breach.

162. As a condition of his employment with Garda, Plaintiff Haley provided Garda with his PII/PHI. Garda required Plaintiff Haley to provide his PII/PHI in order to obtain employment and payment for that employment, and used that PII/PHI to facilitate its employment of Plaintiff Haley, including payroll.

163. Plaintiff Haley provided his PII/PHI to Garda and trusted the company would use reasonable measures to protect it according to Garda's internal policies, as well as state and federal law. Garda obtained and continues to maintain Plaintiff Haley's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

164. Plaintiff Haley reasonably understood that a portion of the funds derived from his employment would be used to pay for adequate cybersecurity and protection of PII/PHI.

165. Plaintiff Haley received a Notice of Data Breach from Garda dated March 22, 2024.

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

167. Through its Data Breach, Garda compromised Plaintiff Haley's PII/PHI, which upon information and belief includes his name, Social Security number, driver's license number, date of birth, and/or insurance, benefit, or other health-related information.

168. Plaintiff Haley has spent, and will continue to spend, significant time and effort monitoring his accounts to protect himself from identity theft due to the Data Breach. After all, Garda directed Plaintiff Haley to take those steps in its Notice of Data Breach. As Plaintiff Haley works sixteen hour shifts, this time spent mitigating effects of the Data Breach takes away from the little time he has to spend on personal matters, which would not be necessary but for the Data Breach.

169. In the aftermath of the Data Breach, Plaintiff Haley has suffered from a spike in spam and scam phone calls.

170. In addition, following the Data Breach Plaintiff Haley received a fraud alert from Experian and was notified about an account inquiry being submitted in his name by an unknown actor without Plaintiff Haley's authorization.

171. Plaintiff Haley fears for his personal financial security and worries about fraudulent use of his information exposed in the Data Breach.

172. Because of Garda's Data Breach, Plaintiff Haley has suffered, and will continue to suffer, anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Haley's injuries are precisely the type of injuries that the law contemplates and addresses.

173. Plaintiff Haley suffered actual injury from the exposure and theft of his PII/PHI, which violates his rights to privacy.

174. Plaintiff Haley suffered actual injury by being deprived of the benefit of the bargain (vis-à-vis his employment with Garda).

175. Plaintiff Haley suffered actual injury in the form of damages to and diminution in the value of his PII/PHI. After all, PII/PHI is a form of intangible property—property that Garda was required to adequately protect.

176. Plaintiff Haley suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Garda's Data Breach placed Plaintiff Haley's PII/PHI right in the hands of criminals.

177. Because of the Data Breach, Plaintiff Haley has spent, and anticipates spending in the future, considerable amounts of time and money to try and mitigate his injuries.

178. Today, Plaintiff Haley has a continuing interest in ensuring that his PII/PHI—which, upon information and belief, remains backed up in Garda’s possession—is protected and safeguarded from additional breaches.

Plaintiffs and Class Members Face Significant Risk of Continued Identity Theft

179. Because of Garda’s failure to prevent the Data Breach, Plaintiffs and Class Members suffered and will continue to suffer damages. These damages include, *inter alia*, monetary losses, lost time, heightened risk of identity theft and/or actual identity theft, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

- a. loss of the opportunity to control how their PII/PHI is used;
- b. diminution in value of their PII/PHI;
- c. compromise and continuing publication of their PII/PHI;
- d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;
- e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;
- f. delay in receipt of tax refund monies;
- g. unauthorized use of their stolen PII/PHI; and
- h. continued risk to their PII/PHI—which remains in Garda’s possession—and is thus as risk for futures breaches so long as Garda fails to take appropriate measures to protect the PII/PHI.

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

181. The value of Plaintiffs and Class's PII/PHI on the black market is considerable. Stolen PII/PHI trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the Dark Web, further exposing the sensitive information.

182. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell Plaintiffs' and Class Members' PII/PHI far and wide.

183. One way criminals profit from stolen PII/PHI is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen PII/PHI, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

184. The development of Fullz packages means that PII/PHI exposed in the Data Breach can be easily linked to Plaintiffs' and Class Members' data that is available on the internet.

185. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII/PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and Class Members' stolen PII/PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

186. Indeed, certain Plaintiffs' stolen PII/PHI has **already** been published on the Dark Web and/or misused for fraudulent and unauthorized transactions.

187. Garda disclosed Plaintiffs' and Class Members' PII/PHI for criminals to use in the conduct of illegal activity. Specifically, Garda opened up, disclosed, and exposed Plaintiffs' and

Class Members' PII/PHI to people engaged in disruptive and unlawful practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open financial accounts in Plaintiffs' and Class Members' names (i.e., identity fraud), all using the PII/PHI stolen in the Data Breach.

188. Garda's failure to promptly and properly notify Plaintiffs and Class Members of the Data Breach exacerbated their injuries by depriving them of the earliest ability to take appropriate measures to protect their PII/PHI or promptly take necessary steps to mitigate the harm caused by the Data Breach.

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

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

190. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.²⁹

191. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."³⁰

192. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Garda's industry, including Defendant.

²⁹ See 2021 Data Breach Annual Report, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) <https://notified.idtheftcenter.org/s/>.

³⁰ Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware>.

Garda Failed to Follow FTC Guidelines

193. According to the Federal Trade Commission (“FTC”), the need for data security should factor into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Garda—should use to protect against unlawful data exposure.

194. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.³¹ The FTC declared that, *inter alia*, businesses must:

- a. protect the personal customer information that they keep;
- b. properly dispose of personal information that is no longer needed;
- c. encrypt information stored on computer networks;
- d. understand their network’s vulnerabilities; and
- e. implement policies to correct security problems.

195. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

196. Furthermore, the FTC explains that companies must

- a. not maintain information longer than is needed to authorize a transaction;
- b. limit access to sensitive data;
- c. require complex passwords to be used on networks;
- d. use industry-tested methods for security;
- e. monitor for suspicious activity on the network; and

³¹ *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

- f. verify that third-party service providers use reasonable security measures.

197. The FTC brings enforcement actions against businesses for failing to protect individuals' personal data adequately and reasonably. Thus, the FTC treats the failure to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45 *et seq.* Enforcement orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

198. In short, Garda's failure to use reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' PII/PHI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Garda Failed to Follow Industry Standards

199. Several best practices have been identified that, at a *minimum*, should be implemented by businesses like Garda. These industry standards include education for all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

200. Other industry standard best practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protecting against any possible communication system; and training staff regarding critical points.

201. Garda failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

202. These frameworks are applicable and accepted industry standards. By failing to comply with these accepted standards, Garda opened the door to criminals accessing Plaintiffs' and Class Members' PII/PHI, thereby causing the Data Breach.

Garda Violated HIPAA

203. The Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d ("HIPAA") circumscribes security provisions and data privacy responsibilities designed to keep individuals' health information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.³²

204. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII/PHI is properly maintained.³³

³² HIPAA lists eighteen types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

³³ See 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

205. The Data Breach itself resulted from a combination of inadequacies showing Garda failed to comply with safeguards mandated by HIPAA. Garda's security failures include, but are not limited to the following:

- a. failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);
- b. failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- c. failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- d. failing to ensure compliance with HIPAA security standards by Garda's workforce in violation of 45 C.F.R. § 164.306(a)(4);
- e. failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- f. failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);
- g. failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);
- h. failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and
- i. failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

206. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Garda failed to comply with safeguards mandated by HIPAA regulations.

CLASS ACTION ALLEGATIONS

207. Plaintiffs bring this class action under Federal Rule of Civil Procedure 23(a), 23(b)(2), and 23(b)(3), on behalf of all members of the following classes (collectively, “Class”):³⁴

Nationwide Class

All individuals residing in the United States whose PII/PHI was compromised in the Data Breach discovered by Garda in November 2023, including all those individuals who received notice of the breach (the “Nationwide Class”).

Illinois Subclass

All individuals residing in Illinois whose PII/PHI was compromised in the Data Breach discovered by Garda in November 2023, including all those individuals who received notice of the breach (the “Illinois Subclass”).

Louisiana Subclass

All individuals residing in Louisiana whose PII/PHI was compromised in the Data Breach discovered by Garda in November 2023, including all those individuals who received notice of the breach (the “Louisiana Subclass”).

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

209. Certification of Plaintiffs’ claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

³⁴ Plaintiffs reserve the right to amend the Class definition.

210. Ascertainability. All members of the proposed Class are readily ascertainable from information in Garda's custody and control. After all, Garda already identified at least some Class Members and sent them its Notice of Data Breach.

211. Numerosity. The Class members are so numerous that joinder of all Class Members is impracticable. Upon information and belief, the proposed Class includes at least 39,928 individuals.

212. Typicality. Plaintiffs' claims are typical of Class Members' claims as each arises from the same Data Breach, the same alleged violations by Garda, and the same unreasonable manner of notifying affected individuals about the Data Breach.

213. Adequacy. Plaintiffs will fairly and adequately protect the proposed Class's common interests. Plaintiffs' interests do not conflict with Class Members' interests. Plaintiffs have retained counsel, including lead counsel, experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

214. Commonality and Predominance. Plaintiffs' and the Class's claims raise common fact and legal questions that predominate over any questions affecting individual Class members, for which a class-wide proceeding can answer for all Class Members. In fact, a class-wide proceeding is necessary to answer the following questions, *inter alia*:

- a. whether Garda had a duty to use reasonable care in safeguarding Plaintiffs' and Class Members' PII/PHI;
- b. whether Garda failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. whether Garda was negligent in maintaining, protecting, and securing Plaintiffs' and Class Members' PII/PHI;
- d. whether Garda breached contractual promises to safeguard Plaintiffs' and Class Members' PII/PHI;

- e. whether Garda took reasonable measures to determine the extent of the Data Breach after discovering it;
- f. whether Garda's Notice of Data Breach was reasonable;
- g. whether the Data Breach caused Plaintiffs and Class Members injuries;
- h. whether Plaintiffs and the Class are entitled to damages, treble damages, and or injunctive relief; and
- i. the proper measure of damages measure is.

215. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members are relatively small compared to the burden and expense that individual litigation against Garda would require. Thus, it would be practically impossible for each Class Member, to obtain effective redress for his or her injuries on an individual basis. Not only would individualized litigation increase the delay and expense to all parties and the courts, but it would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

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

216. Plaintiffs incorporate by reference paragraphs 1–212 as if fully set forth herein.

217. Plaintiffs and Class Members (or their third-party agents) entrusted their PII/PHI to Garda on the premise and with the understanding that Garda would safeguard their PII/PHI, use

their PII/PHI for legitimate business purposes only, and/or not disclose their PII/PHI to unauthorized parties.

218. Garda owed a duty of care to Plaintiffs and Class Members because it was foreseeable that Garda's failure to use adequate data security in accordance with industry standards for data security would cause a data breach that compromises Plaintiffs' and Class Members' PII/PHI.

219. Garda has full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiffs and Class Members' could and would suffer if their PII/PHI was wrongfully disclosed.

220. Garda owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable group of individuals whom Garda knew or should have known would suffer injuries from Garda's inadequate data security practices. After all, Garda actively sought and obtained Plaintiffs and Class Members' PII/PHI.

221. Garda' owed Plaintiffs and Class Members at least the following duties:

- a. to exercise reasonable care in handling and using the PII/PHI in its care and custody;
- b. to implement industry-standard security procedures sufficient to reasonably protect Plaintiffs' and Class Members' PII/PHI from a data breach, theft, and unauthorized access;
- c. to promptly detect attempts at unauthorized access of PII/PHI in its custody;
- d. to notify Plaintiffs and Class Members within a reasonable time of any breach to the security of their PII/PHI.

222. Garda further owed the duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and occurrence of the Data Breach, which disclosure is required and necessary for Plaintiffs and Class Members to take appropriate measures to protect their PII/PHI,

to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate harm caused by the Data Breach.

223. Garda also had a duty to exercise appropriate clearinghouse practices to delete PII/PHI it was no longer required to retain under applicable regulations.

224. Garda knew or reasonably should have known that its failure to exercise due care in the collecting, storing, and using of Plaintiffs' and Class Members' PII/PHI created an unreasonable risk of harm to Plaintiffs and Class Members, in that such failure would unreasonably expose Plaintiffs and Class Members to harms caused by criminal acts of third party hackers.

225. Garda's duty to use reasonable security measures further arose because of the special relationship that existed between Garda on one hand and Plaintiffs and Class Members on the other. That special relationship arose because Plaintiffs and Class Members (or their third-party agents) entrusted Garda with their confidential PII/PHI, a necessary part of obtaining services and/or employment from Garda.

226. Under the FTCA, 15 U.S.C. § 45, Garda had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' PII/PHI.

227. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Garda of failing to use reasonable measures to protect the PII/PHI entrusted to them. FTC publications and orders promulgated pursuant to the FTCA also form part of the basis of Garda's duty to protect Plaintiffs and Class Members' sensitive PII/PHI.

228. Garda violated its duties under Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiffs' and Class Members' PII/PHI and not complying with applicable industry standards as described in detail herein. Garda's conduct was particularly unreasonable

given the nature and amount of PII/PHI it had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

229. Similarly, under HIPAA, Garda had a duty to follow HIPAA standards for privacy and security practices to protect Plaintiffs' and Class Members' PHI.

230. Garda violated its duty under HIPAA by failing to use reasonable measures to protect Plaintiffs' and Class Members' PHI and by not complying with applicable regulations detailed *supra*. Garda's conduct was particularly unreasonable given the nature and amount of PHI that it collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

231. The risk that unauthorized persons would attempt to gain access to Plaintiffs' and Class Members' PII/PHI and misuse it was reasonably foreseeable to Garda. Given that Garda holds vast amounts of PII/PHI, it was inevitable that unauthorized individuals would attempt to access Garda's network systems containing Plaintiffs' and Class Members' PII/PHI, whether by malware or otherwise.

232. PII/PHI is highly valuable, and Garda knew, or should have known, the risk in obtaining, using, handling, emailing, and storing Plaintiffs' and Class Members' PII/PHI and the importance of exercising reasonable care in doing so.

233. Garda improperly and inadequately safeguarded Plaintiffs' and Class Members' PII/PHI in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

234. Garda breached its duties of care owed to Plaintiffs and Class Members by failing to take reasonable steps to protect their PII/PHI from disclosure, as evidenced by the Data Breach.

235. Garda further breached its duties of care owed to Plaintiffs and Class Members by failing to timely notify them their sensitive PII/PHI was compromised in the Data Breach, instead waiting *five months* after discovering the Data Breach to notify Plaintiffs and Class Members.

236. Garda acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class Members' PII/PHI by, *inter alia*,

- a. disclosing and providing access to this information to third parties; and
- b. failing to properly supervise both the way the PII/PHI was stored, used, and exchanged, and its employees who were responsible for those activities.

237. Garda additionally breached its duties of care owed to Plaintiffs and Class Members by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing Plaintiffs' and Class Members' PII/PHI, which directly and proximately caused the Data Breach and Plaintiffs and Class members' injury.

238. Garda further breached its duties of care owed to Plaintiffs and Class Members by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs and Class Members' resulting injuries.

239. Garda has admitted that the PII/PHI of Plaintiffs and the Class was wrongfully accessed and disclosed to unauthorized hackers in the Data Breach.

240. And, on information and belief, Plaintiffs' and Class Members' PII/PHI has already been published, or will be published imminently, by cybercriminals on the Dark Web.

241. As a direct and proximate result of Garda's negligent breaches of its duties of care owed to Plaintiffs and Class Members, Plaintiffs and Class Members have suffered and will continue to suffer injuries and consequential damages, including monetary damages, lost time, increased risk of future harm including identity theft, actual identity theft, and emotional distress.

242. But for Garda's breaches of its duties of care owed to Plaintiffs' and Class Members, the Data Breach the injuries and damages to Plaintiffs and Class Members that resulted would not have occurred.

243. Garda's breach of its duties to exercise reasonable care as set forth above actually and proximately caused Plaintiffs and Class Members actual, tangible, injuries-in-fact and damages, including, without limitation, the theft of their PII/PHI by criminals, improper disclosure of their PII/PHI, lost benefit of their bargain, lost value of their PII/PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Garda's negligence, which injuries and damages are ongoing, imminent, immediate, will last for Plaintiffs' and Class Members' respective lifetimes.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

244. Plaintiffs incorporate by reference paragraphs 1–212 as if fully set forth herein.

245. Plaintiffs and Class Members either directly contracted with Garda or were the third-party beneficiaries of contracts with Garda.

246. Plaintiffs and Class Members (or their third-party agents) were required to provide their PII/PHI to Garda as a condition of receiving products, services, and/or employment from Garda. Plaintiffs and Class Members (or their third-party agents) provided their PII/PHI to Garda or its third-party agents in exchange for Garda's products, services, and/or employment.

247. Plaintiffs and Class Members (or their third-party agents) reasonably understood that a portion of the funds they paid (or funds derived from their labor with) Garda would be used to pay for adequate cybersecurity measures.

248. Plaintiffs and Class Members (or their third-party agents) reasonably understood that Garda would use adequate cybersecurity measures to protect the PII/PHI that Plaintiffs and Class Members (or their third-party agents) were required to provide based on Garda's duties under state and federal law and its internal policies.

249. Plaintiffs and the Class Members (or their third-party agents) accepted Garda's offers by disclosing their PII/PHI to Garda in exchange for receiving products, services, and/or employment from Garda.

250. In turn, and through internal policies, Garda agreed to implement reasonable data security measures and to protect and not disclose Plaintiffs' and Class Members' PII/PHI to unauthorized persons.

251. In its Privacy Policy, Garda promised to undertake adequate measures to protect Plaintiffs' and Class Members' PII/PHI.

252. Implicit in Plaintiffs' and Class Members' agreement was that Garda would provide Plaintiffs and Class Members (or their third-party agents) with prompt and adequate notice of all unauthorized access and/or theft of their PII/PHI.

253. Plaintiffs and Class Members (or their third-party agents) would not have entrusted their PII/PHI to Garda (or their third-party agents) in the absence of Garda's agreement to adequately protect that information from unauthorized disclosure.

254. Plaintiffs and Class Members (or their third-party agents) fully performed their obligations under their implied contracts with Garda, or such performance was waived by Garda's conduct.

255. The covenant of good faith and fair dealing is an element of every contract. Thus, contract parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit, and not merely the letter, of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

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

257. Garda materially breached the contracts it entered with Plaintiffs and Class Members (or their third-party agents) by the following acts and omissions:

- a. failing to safeguard Plaintiffs' and Class Members' PII/PHI;
- b. failing to notify Plaintiffs and Class Members promptly of the intrusion into Garda's computer systems that compromised their PII/PHI;
- c. failing to comply with industry standards for securing PII/PHI;
- d. failing to comply with legal obligations necessarily incorporated into its agreements with Plaintiffs and Class Members (or their third-party agents); and
- e. failing to ensure the confidentiality and integrity of Plaintiffs' and Class Members' PII/PHI that Garda created, received, maintained, and transmitted.

258. In these and other ways, Garda violated its duty of good faith and fair dealing.

259. Garda's material breaches were the direct and proximate cause of Plaintiffs' and Class Members' injuries and resulting damages, as detailed *supra*.

THIRD CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

260. Plaintiffs incorporate by reference paragraphs 1–212 as if fully set forth herein.

261. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their highly sensitive and confidential PII/PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

262. Garda owed a duty to its current and former employees and/or customers, including Plaintiffs and Class Members, to keep the PII/PHI it collected and maintained confidential and protected from unauthorized disclosure.

263. The unauthorized acquisition (i.e., theft) of Plaintiffs and Class Members' PII/PHI by a criminal organization is highly offensive to a reasonable person.

264. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and Class Members (or their third-party agents) disclosed their sensitive and confidential PII/PHI to Garda privately and with the intention that such information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private by Garda, a sophisticated business entity in the security business itself, and would not be disclosed without their authorization.

265. The Data Breach constitutes an intentional interference with Plaintiffs' and Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

266. Garda acted with a knowing state of mind when it permitted the Data Breach

because it knew its information security practices were inadequate.

267. Garda acted with a knowing state of mind when it failed to notify Plaintiffs and Class Members in a timely fashion about the Data Breach, thereby materially impairing their efforts to mitigate harm caused by the Data Breach.

268. Garda had notice and knew that its inadequate cybersecurity practices would cause injuries to Plaintiffs and Class Members.

269. As a direct and proximate result of Garda's acts and omissions, Plaintiffs' and Class Members' private and sensitive PII/PHI of was stolen by a criminal hacking organization and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and Class Members to suffer injuries and consequential damages, as detailed *supra*.

270. And, on information and belief, Plaintiffs' and Class Members' PII/PHI compromised in the Data Breach has already been published, or will be published imminently, by cybercriminals on the Dark Web.

271. Unless and until enjoined and restrained by order of this Court, Garda's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members because their PII/PHI is still maintained by Garda with their inadequate cybersecurity system and policies.

272. Plaintiffs and Class Members have no adequate remedy at law for their injuries tied to Garda's continued possession of their sensitive and confidential PII/PHI. A judgment for monetary damages will not end Garda's inability to safeguard Plaintiffs' and Class Members' PII/PHI in its custody.

273. In addition to injunctive relief, Plaintiffs, on behalf of themselves and Class Members, also seek compensatory damages for Garda's invasion of privacy, which includes the

value of the privacy interest invaded by Garda, the costs of future monitoring of their credit history for identity theft and fraud, along with prejudgment interest and costs.

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

274. Plaintiffs incorporate by reference paragraphs 1–212 as if fully set forth herein.

275. This claim is pleaded in the alternative to Plaintiffs’ breach of implied contract cause of action.

276. Plaintiffs and Class Members (or their third-party agents) conferred a benefit upon Garda, in that Garda benefitted from collecting and using Plaintiffs’ and Class Members’ PII/PHI and labor to provide services and/or facilitate employment.

277. Garda appreciated and knew of the benefits it received from Plaintiffs and Class Members (or their third-party agents).

278. Plaintiffs and Class Members (or their third-party agents) reasonably expected that Garda would use adequate cybersecurity measures to protect the PII/PHI they were required to provide based on Garda’s duties under state and federal law and its internal policies.

279. Garda enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs’ and Class Members’ PII/PHI.

280. Instead of providing a reasonable level of data security that would have prevented the Data Breach, Garda instead calculated to avoid its data security obligations at Plaintiffs’ and Class Members’ expense by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, were injured as a direct and proximate result of Garda’s failure to provide the requisite security, which caused the Data Breach.

281. Under principles of equity and good conscience, Garda should not be permitted to

retain the full value of Plaintiffs' and Class Members' employment and/or payment because Garda failed to take reasonable and required steps to adequately protect Plaintiffs' and Class Members' PII/PHI.

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

283. Garda should be compelled to disgorge all unlawful or inequitable proceeds that it received because of its misconduct into a common fund for the benefit of Plaintiffs and Class Members.

FIFTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

284. Plaintiffs incorporate by reference paragraphs 1–212 as if fully set forth herein.

285. Given the relationship between Garda, on one hand, and Plaintiffs and Class Members, on the other hand, wherein Garda served as guardian of Plaintiffs' and Class Members' PII/PHI, Garda became a fiduciary by its undertaking to collect and maintain that PII/PHI.

286. As Plaintiffs' and Class Members' fiduciary, Garda was obligated to act primarily for Plaintiffs and Class Members (a) to safeguard of Plaintiffs and Class Members' PII/PHI in its custody; (b) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure of their PII/PHI; and (c) to maintain complete and accurate records of what information (and where) Garda did and does store.

287. Garda had and has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Garda's relationship with them—especially to secure their PII/PHI.

288. Because of the highly sensitive nature of the PII/PHI they provided to Garda, Plaintiffs and Class Members (or their third-party agents) would not have entrusted Garda, or

anyone in Garda's position, to retain their PII/PHI had they known the reality of Garda's inadequate data security practices.

289. Garda breached its fiduciary duties to Plaintiffs and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class Members' PII/PHI from unauthorized disclosure.

290. Garda also breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

291. As a direct and proximate result of Garda's breaches of fiduciary duties owed to Plaintiffs and Class Members, Plaintiffs' and Class Members' sensitive PII/PHI was accessed and exposed through the Data Breach.

292. As a direct and proximate result of Garda's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer numerous injuries and consequential damage, as detailed *supra*.

SIXTH CAUSE OF ACTION

Violation of Florida Deceptive and Unfair Trade Practices Act

Fla. Stat. § 501.201, *et seq.*

(On Behalf of Plaintiffs and the Class)

293. Plaintiffs incorporate by reference paragraphs 1–212 as if fully set forth herein.

294. This cause of action is brought under the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), section 501.201, Florida Statutes, *et seq.*

295. The purpose of FDUTPA is to "protect the consuming public and legitimate business enterprises from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce." Fla. Stat. § 501.202(2).

296. Another purpose of FDUTPA is to construe consumer protection as “consistent with established policies of federal law relating to consumer protection.” Fla. Stat. § 501.202(3).

297. Plaintiffs and Class members all constitute “consumers” under FDUTPA because they are all “individual[s].” Fla. Stat. § 501.203.

298. Plaintiffs and Class members each constitute an “interested party or person” under FDUTPA because they are all “affected by a violation” of FDUTPA. Fla. Stat. § 501.203.

299. FDUTPA applies to Garda because Garda engages in “trade or commerce,” which FDUTPA defines as “advertising, soliciting, providing, offering, or distributing, whether by sale, rental, or otherwise, of any good or service, or any property, whether tangible or intangible, or any other article, commodity, or thing of value, wherever situated.” Fla. Stat. § 501.203.

300. FDUTPA declares unlawful “unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce.” Fla. Stat. § 501.204(1).

301. FDUTPA provides that “due consideration be given to the interpretations of the Federal Trade Commission and the federal courts relating to Section 5(a)(1) of the Trade Commission Act.” Fla. Stat. § 501.204(2).

302. Relevant here, is that “[v]iolation[s]” of FDUTPA are broadly defined to include violations of:

- a. “Any rules promulgated pursuant to the Federal Trade Commission Act, 15 U.S.C. ss. 41 *et seq.*” Fla. Stat. § 501.203.
- b. “The standards of unfairness and deception set forth and interpreted by the Federal Trade Commission or the federal courts.” Fla. Stat. § 501.203.
- c. “Any law, statute, rule, regulation, or ordinance which proscribes unfair methods of competition, or unfair, deceptive, or unconscionable acts or practices.” Fla. Stat. § 501.203.

303. Under FCRA, HIPAA, the FTCA, and Florida law (Fla. Stat. §§ 456.057, 501.171), Garda was required to implement adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiffs' and Class Members' PII/PHI. Garda also had the \ express obligation under Florida law, the state where Garda is headquartered and managed, to adequately protect Plaintiffs' and Class Members' PII/PHI.

304. Moreover, FDUTPA requires that Garda (a) take reasonable measures to protect and secure data in electronic form containing PII/PHI; (b) take reasonable measures to dispose of or destroy PII/PHI; and (c) provide notice to consumers and consumer reporting agencies subject to the FCRA when a data security incident occurs that compromises PII/PHI. Fla. Stat. § 501.171.

305. Garda violated FDUTPA by, *inter alia*,

- a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' PII/PHI, which was a direct and proximate cause of the Data Breach;
- b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII/PHI, including duties imposed by the FTCA and HIPAA, which was a direct and proximate cause of the Data Breach;
- d. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' PII/PHI; and
- e. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII/PHI, including duties imposed by the FTCA and HIPAA.

306. Garda's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Garda's data security and ability to protect the confidentiality of PII/PHI.

307. Garda intended to mislead Plaintiffs and Class Members and induce them to rely on its omissions.

308. Plaintiffs and Class Members did rely on Garda's misleading statements and/or omissions in providing their PII/PHI to Garda, and would not have done so had they known the truth of Garda's inadequate data security practices.

309. Had Garda disclosed to Plaintiffs and Class Members (or their third-party agents) that its data systems were not secure and thus vulnerable to attack, Garda would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law. Garda accepted the PII/PHI that Plaintiffs and Class Members (or their third-party agents) entrusted to it while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and Class Members acted reasonably in relying on Garda's misleading statements and/or omissions, the truth of which they could not have discovered through reasonable investigation.

310. Garda acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiffs' and Class Members' rights.

311. As a direct and proximate result of Garda's unfair and deceptive acts and practices, Plaintiffs and Class Members have suffered and will continue to suffer such injuries as ascertainable losses of money or property; monetary and non-monetary damages, including from fraud and identity theft; loss of time and expenses related to monitoring their financial accounts

for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII/PHI.

312. And, on information and belief, Plaintiffs' and Class Members' PII/PHI stolen in the Data Breach has already been published, or will be published imminently, by cybercriminals on the Dark Web.

313. Plaintiffs and Class Members seek declaratory judgement that Garda's practices were unreasonable and inadequate and thus caused the Data Breach.

314. Plaintiffs and Class Members seek injunctive relief enjoining the wrongful acts described *supra* and requiring Garda to use and maintain proper standards for data security including, inter alia, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing. *See* Fla. Stat. § 501.211(1).

315. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including seek actual damages, attorneys' fees, and costs pursuant to FDUPTA.

SEVENTH CAUSE OF ACTION
Violation of the Louisiana Database Security Breach Notification Law
La. Stat. Ann. §§ 51:3071 *et seq.*
(On Behalf of Plaintiff Jeremy Angelle and the Louisiana Subclass)

316. Plaintiff Jeremy Angelle incorporates by reference paragraphs 1–212 as if fully set forth herein.

317. As stated by the Louisiana Legislature, the purpose of the Louisiana Database Security Breach Notification Law ("LDSBNL") is to address the following issues:

- a. "The privacy and financial security of individuals are increasingly at risk due to the ever more widespread collection of personal information." La. Stat. Ann. § 51:3072(1).

- b. “The crime of identity theft is on the rise in the United States.” *Id.* § 51:3072(3).
- c. “Criminals who steal personal information use the information to open credit card accounts, write bad checks, buy automobiles, and commit other financial crimes using the identity of another person.” *Id.*
- d. “Identity theft is costly to the marketplace and to consumers.” *Id.* § 51:3072(4).
- e. “Victims of identity theft must act quickly to minimize the damage; therefore, expeditious notification of possible misuse of a person’s personal information is imperative.” *Id.* § 51:3072(5).

318. Thus, the LDSBNL provides, *inter alia*, that:

- a. “Any person that conducts business in the state or that owns or licenses computerized data that includes personal information . . . **shall implement and maintain reasonable security procedures and practices** appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.” *Id.* § 51:3074(A) (emphasis added).
- b. “Any person that conducts business in the state or that owns or licenses computerized data that includes personal information . . . **shall take all reasonable steps to destroy or arrange for the destruction of the records** within its custody or control containing personal information that is no longer to be retained by the person or business by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.” *Id.* § 51:3074(B) (emphasis added).
- c. “Any person that owns or licenses computerized data that includes personal information . . . shall, following discovery of a breach in the security of the system containing such data, notify any resident of the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.” *Id.* § 51:3074(C). And “[t]he **notification required . . . shall be made** in the most expedient time possible and without unreasonable delay but **not later than sixty days from the discovery of the breach**[.]” *Id.* § 51:3074(E) (emphasis added).

319. As such, the LDSBNL establishes that “[a] civil action may be instituted to recover actual damages[.]” *Id.* § 51:3075.

320. This Data Breach constitutes a “[b]reach of the security of the system” because this Data Breach caused the “compromise of the security, confidentiality, or integrity of computerized data[.]” *Id.* § 51:3073(2).

321. Plaintiff Jeremy Angelle, Louisiana Subclass Members, and Garda are all “person[s]” because they are either an “individual, corporation, partnership, sole proprietorship, joint stock company, joint venture, or any other legal entity.” *Id.* § 51:3073(3).

322. The exposed PII/PHI constitutes “[p]ersonal information” because the exposed PII/PHI includes, *inter alia*, unredacted and/or unencrypted names, Social Security numbers, and driver’s license numbers. *Id.* § 51:3073(4)(a).

323. Notably, the LDSBNL provides that “[a] violation of a provision of this Chapter shall constitute an unfair act or practice[.]” *Id.* § 51:3074(J).

324. Here, Garda violated the LDSBNL by, *inter alia*:

- a. failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the PII/PHI to protect the PII/PHI to from unauthorized access, destruction, use, modification, or disclosure;
- b. failing to take all reasonable steps to destroy or arrange for the destruction of Plaintiff Angelle’s and Louisiana Subclass Members’ records within its custody or control containing PII/PHI to that is no longer to be retained by the person or business by shredding, erasing, or otherwise modifying the PII/PHI to in the records to make it unreadable or undecipherable through any means; and
- c. failing to provide notification in the most expedient time possible and without unreasonable delay—instead waiting 127 days after discovery of the Data Breach (which far exceeds the sixty-day deadline of the LDSBNL) to notify Plaintiff Angelle and Louisiana Subclass Members that their PII/PHI was compromised.

325. As a direct and proximate result of Garda's violations of the LDSBNL, Plaintiff Angelle and Louisiana Subclass Members have suffered and will continue to suffer injuries including ascertainable losses of money or property; monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII/PHI.

326. And, on information and belief, Plaintiff Angelle's and Louisiana Subclass Members' PII/PHI has already been published, or will be published imminently, by cybercriminals on the Dark Web.

327. Plaintiff and Louisiana Subclass Members seek all monetary and non-monetary relief allowed by law.

EIGHTH CAUSE OF ACTION
Violation Of The Illinois Consumer Fraud Act
815 Ill. Comp. Stat. §§ 505/1, *et seq.*
(On Behalf of Plaintiff Ryan Gawronski and the Illinois Subclass)

328. Plaintiff Ryan Gawronski incorporates by reference paragraphs 1–212 as if fully set forth herein.

329. This claim is brought under the Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA").

330. Plaintiff Ryan Gawronski and Illinois Subclass Members are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e).

331. Plaintiff Gawronski, the Illinois Subclass, and Garda are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

332. The ICFA applies to Garda because Garda engages in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Garda engages

in the sale of “merchandise” (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b), (d).

333. Garda violated the ICFA by, *inter alia*:

- a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Gawronski’s and Illinois Subclass Members’ PII/PHI, which was a direct and proximate cause of the Data Breach;
- b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Gawronski’s and Illinois Subclass Members’ PII/PHI, including duties imposed by the FTCA and HIPAA, which was a direct and proximate cause of the Data Breach;
- d. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Gawronski’s and Illinois Subclass Members’ PII/PHI; and
- e. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Gawronski’s and Illinois Subclass Members’ PII/PHI, including duties imposed by the FTCA and HIPAA.

334. Garda’s omissions were material because they were likely to deceive reasonable consumers about the adequacy of Garda’s data security and ability to protect the confidentiality of Plaintiff Gawronski’s and Illinois Subclass Members’ PII/PHI.

335. Garda intended to mislead Plaintiff Gawronski and Illinois Subclass Members and induce them to rely on its omissions.

336. Plaintiff Gawronski and Illinois Subclass Members did rely on Garda’s misleading statements and/or omissions in providing their PII/PHI to Garda, and would not have done so had they known the truth of Garda’s inadequate data security practices.

337. Had Garda disclosed to Plaintiff Gawronski and Illinois Subclass Members (or their third-party agents) that its data systems were not secure and thus vulnerable to attack, Garda would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Garda accepted the PII/PHI that Plaintiff Gawronski and Illinois Subclass Members (or their third-party agents) entrusted to it while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff Gawronski and Illinois Subclass Members acted reasonably in relying on Garda's omissions, the truth of which they could not have discovered through reasonable investigation.

338. Garda acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiff Gawronski's and Illinois Subclass Members' rights.

339. As a direct and proximate result of Garda's unfair and deceptive acts and practices, Plaintiff Gawronski and Illinois Subclass Members have suffered and will continue to suffer injuries including ascertainable losses of money or property; monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII/PHI.

340. And, on information and belief, Plaintiff Gawronski's and Illinois Subclass Members' PII/PHI has already been published, or will be published imminently, by cybercriminals on the Dark Web.

341. Plaintiff Gawronski and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law.

342. Garda's wrongful practices were and are injurious to the public because those practices were part of Garda's generalized course of conduct that applied to the Illinois Subclass

as a whole. Plaintiff Gawronski and Illinois Subclass Members have been adversely affected by Garda's conduct and the public was and is at risk as a result thereof.

343. Garda also violated 815 ILCS 505/2 by failing to immediately notify Plaintiff Gawronski and Illinois Subclass Members of the nature and extent of the Data Breach pursuant to the Illinois PII Protection Act, 815 ILCS 530/1, *et seq.*

344. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff Gawronski and Illinois Subclass Members seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Garda's violations of the ICFA.

NINTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiffs and the Class)

345. Plaintiffs incorporate by reference paragraphs 1–212 as if fully set forth herein.

346. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

347. In the fallout of the Data Breach, an actual controversy has arisen about Garda's various duties to use reasonable data security. On information and belief, Plaintiffs allege that Garda's actions were—and *still* are—inadequate and unreasonable. Plaintiffs and Class Members continue to suffer injury from the ongoing threat of fraud and identity theft.

348. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- a. Garda owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

- b. Garda has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTCA;
- c. Garda breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and
- d. Garda breaches of its duties caused—and continues to cause—injuries to Plaintiffs and Class Members.

349. The Court should also issue corresponding injunctive relief requiring Garda to use adequate security consistent with industry standards to protect the data entrusted to it.

350. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injuries and lack an adequate legal remedy if Garda experiences a second data breach.

351. And if a second breach occurs, Plaintiffs and Class Members will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted for out-of-pocket damages and other legally quantifiable and provable damages, cannot cover the full extent of Plaintiffs and Class Members' injuries.

352. If an injunction is not issued, the resulting hardship to Plaintiffs and Class Members far exceeds the minimal hardship that Garda could experience if an injunction is issued.

353. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiffs, Class Members, and the public at large.

PRAYER FOR RELIEF

Plaintiffs and Class Members respectfully request that the Court enter judgment against Garda and an order as follows:

- A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

- B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiffs and the Class;
- C. Awarding injunctive relief as necessary to protect the interests of Plaintiffs and the Class;
- D. Enjoining Garda from further unfair and/or deceptive practices;
- E. Awarding Plaintiffs and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;
- F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;
- G. Awarding attorneys' fees and costs, as allowed by law;
- H. Awarding prejudgment and post-judgment interest, as provided by law;
- I. Granting all other and further relief that this Court deems appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial for all claims so triable.

Date: May 28, 2024

Respectfully submitted,

By: /s/ John A. Yanchunis

John A. Yanchunis (FL State Bar No. 324681)
Ronald Podolny*
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 North Franklin Street 7th Floor
Tampa, Florida 33602
T: (813) 223-5505
F: (813) 223-5402
jyanchunis@forthepeople.com
ronald.podolny@forthepeople.com

Mariya Weekes (FL State Bar No. 56299)
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
201 Sevilla Avenue, 2nd Floor
Coral Gables, Florida 33134
T: (786) 879-8200

F: (786) 879-7520
mweekes@milberg.com

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

William B. Federman*
FEDERMAN & SHERWOOD
212 W. Spring Valley Road,
Richardson, Texas 75081
T: (405) 235-1560
F: (405) 239-2112
wbf@federmanlaw.com

Steven Sukert*
**KOPELOWITZ OSTROW FERGUSON
WEISELBERG GILBERT**
1 West Las Olas, Suite 500
Fort Lauderdale, Florida 33301
T: (954) 525-4100
F: (954) 525-4300
sukert@kolawyers.com

John G. Emerson*
EMERSON FIRM, PLLC
2500 Wilcrest Drive, Suite 300
Houston, Texas 77042-2754
T: (800) 551-8649
F: (501) 286-4659
jemerson@emersonfirm.com

Raina C. Borrelli*
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
T: (872) 263-1100
F: (872) 263-1109
raina@straussborrelli.com

**Pro hac vice forthcoming*

Attorneys for Plaintiffs and Proposed Class

CERTIFICATE OF SERVICE

I certify that on this 28th day of May, 2024, a true and correct copy of the foregoing was filed with the Clerk of Court via the Court's CM/ECF system for electronic service on all counsel of record.

/s/ John A. Yanchunis

John A. Yanchunis