IN THE UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

DANIEL CUNNINGHAM and DEBRA DE SALVO, *individually and on behalf of all others similarly situated*, Plaintiffs, v. DG3 NORTH AMERICA, INC. d/b/a DIVERSIFIED GLOBAL GRAPHICS GROUP, and JOHN HANCOCK INVESTMENT MANAGEMENT, LLC and UBS FINANCIAL SERVICES, INC., Defendants.	Case No.: 2:24-cv-07385 **AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Daniel Cunningham and Debra De Salvo ("Plaintiffs") bring this Amended Class Action Complaint on behalf of themselves and all others similarly situated (Class Members), against Defendants, DG3 North America, Inc. d/b/a/ Diversified Global Graphics Group ("DG3"), John Hancock Investment Management, LLC ("John Hancock") and UBS Financial Services, Inc. ("UBS") (DG3, UBS, and John Hancock together, "Defendants"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to them, which are based on personal knowledge:

NATURE OF THE CASE

1. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard Plaintiffs' and Class Members' sensitive personally identifying information ("PII"), including full names, addresses, email addresses, investment fund information and account numbers, and Social Security numbers, which as a result, is now in criminal cyberthieves' possession.

2. Defendant John Hancock is an investment advisory firm that provides portfolio management services to individual and institutional clients across the United States.[1]

3. Defendant UBS is a New-Jersey based financial services and insurance company.

4. Defendant DG3 provides communication and marketing services to business clients in various industries,[2] including John Hancock and UBS. In the course of DG3 and UBS and John Hancock's relationship, UBS and John Hancock provide its customers' PII to DG3, and DG3 collects and maintains that information.

5. Plaintiffs and Class Members are current and former clients of John Hancock and/or UBS, who, in order to obtain services from John Hancock and/or UBS, were and are required to entrust Defendants with their sensitive, non-public PII. Defendants could not perform their regular business activities without obtaining Plaintiffs' and Class Members' PII retain this information for many years, at least, even after the customer relationship has ended.

6. Businesses like Defendants that handle PII owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of PII to unauthorized persons—and especially hackers with nefarious intentions—will harm the affected individuals, including, but not limited to, by the invasion of their private financial matters.

7. On or about March 19, 2024, DG3 learned that its computer network systems had experienced a cybersecurity incident. Upon investigating, DG3 confirmed that its network was penetrated by a cyberattack (the "Data Breach"), through which unauthorized criminal hackers

---

[1] *See* Form ADV, John Hancock Invest. Mgmt. LLC, https://files.adviserinfo.sec.gov/IAPD/content/viewform/adv/Sections/iapd_AdvAdvisoryBusinessSection.aspx?ORG_PK=105790&FLNG_PK=056E0AD2000801DD04EC8751053D4705056C8CC0 (last visited June 28, 2024).

[2] *See* About Us, https://dg3.com/about/ (last visited June 28, 2024); Our Solutions, https://dg3.com/solutions/ (last visited June 28, 2024).

accessed and exfiltrated files containing individuals' PII. In or around April 2024, DG3 concluded that Plaintiffs' and Class Members' PII was compromised in the Data Breach.

8. According to DG3's Notice of Data Breach provided to the Attorney General of Montana,[3] the PII compromised in the Data Breach includes full names, addresses, Social Security numbers, and fund and account numbers associated with individual customers' accounts.

9. Despite that Defendants have known about the Data Breach since at least March 19, 2023, DG3 waited nearly three months before notifying Plaintiffs and Class Members their sensitive PII was exposed. To date, neither UBS or John Hancock has provided any notification or information about the Data Breach to Plaintiffs and Class Members.

10. Defendants failed to adequately protect Plaintiffs' and Class Members' PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendants' intentional, reckless, negligent, and/or careless acts and omissions and their utter failure to protect their customers' sensitive data. Hackers targeted and obtained Plaintiffs' and Class Members' PII because of the information's value in exploiting and stealing individuals' identities. The present and continuing risk to Plaintiffs and Class Members as victims of the Data Breach will remain for their respective lifetimes.

11. Defendants maintained the PII in a reckless manner. Specifically, PII was maintained on DG3's computer network in a condition vulnerable to cyberattacks, and UBS and John Hancock permitted such inadequate cybersecurity practices from its vendor. The mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' PII was a known risk to Defendants, and thus, Defendants knew that failing to take reasonable steps to

[3] *See* Notice of Data Breach – Third-party Cybersecurity Incident, https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-1444.pdf (last visited June 28, 2024).

secure the PII left it in a dangerous condition.

12. As a direct and proximate result of Defendants' inadequate data security and breaches of their duties to handle PII with reasonable care, Plaintiffs' and Class Members' PII has been accessed by hackers and exposed to an untold number of unauthorized individuals.

13. The harm resulting from a cyberattack like this Data Breach manifests in numerous ways including identity theft and financial fraud, and the exposure of an individual's PII due to a data breach ensures that the individual will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of his or his life. Mitigating that risk, to the extent it is even possible to do so, requires individuals to devote significant time and money to closely monitor their credit, financial accounts, and email accounts, and take several additional prophylactic measures.

14. As a result of Defendants' conduct and the resulting Data Breach, Plaintiffs and Class Members suffered concrete injuries in fact including, but not limited to (a) identity theft and fraud, or the imminent risk thereof; (b) invasion of privacy; (c) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (d) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (e) financial costs incurred due to actual identity theft; (f) loss of time incurred due to actual identity theft; (g) deprivation of value of their PII; and (h) the continued risk to their sensitive PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII they collect and maintain.

15. To recover from Defendants for these harms, Plaintiffs, on behalf of themselves and the Class as defined herein, bring claims for negligence/negligence *per se*, breach of implied contract, breach of third-party beneficiary contract, breach of fiduciary duty, breach of confidence,

and unjust enrichment to address Defendants' inadequate safeguarding of Plaintiffs' and Class Members' PII they collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and Class Members that their information was subject to the unauthorized access by a notorious ransomware group in the Data Breach.

16. Plaintiffs and Class Members seek compensatory damages, declaratory judgment, and injunctive relief requiring Defendants to (a) disclose, expeditiously, the full nature of the Data Breach and the types of PII obtained exposed; (b) implement improved data security practices to reasonably guard against future breaches of PII possessed by Defendants; and (c) provide, at Defendants' own expense, all impacted victims with lifetime identity theft protection services.

PARTIES

17. Plaintiff Daniel Cunningham is an adult individual who at all relevant times has been a citizen and resident of Anoka, Minnesota.

18. Plaintiff Debra De Salvo is an adult individual who at all relevant times has been a citizen and resident of Elmwood Park, Illinois.

19. Defendant DG3 is a corporation organized under New Jersey law with its principal place of business located at 100 Burma Road, Jersey City, New Jersey 07305.

20. Defendant John Hancock, is a corporation organized under Delaware law with its principal place of business located at 200 Berkeley Street, Boston, Massachusetts 02116.[4]

21. Defendant UBS is a corporation with its principal place of business located in Weehawken, New Jersey.

[4] *See* Items 1, 3, Form ADV, https://files.adviserinfo.sec.gov/IAPD/content/viewform/adv/Sections/iapd_AdvIdentifyingInfoSection.aspx?ORG_PK=105790&FLNG_PK=056E0AD2000801DD04EC8751053D4705056C8CC0# (last visited June 28, 2024).

JURISDICTION AND VENUE

22. 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. The number of Class Members exceeds 100, some of whom have different citizenship from one or both Defendants, including Plaintiffs. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

23. This Court has personal jurisdiction over Defendant DG3 because it is a New Jersey company that operates and is headquartered in this District and conducts substantial business in this District.

24. This Court has personal jurisdiction over Defendant John Hancock because it has sufficient minimal contacts with this State in that it operates and engages in business in New Jersey, has physical offices in New Jersey, and Plaintiffs' causes of action arise out of and relate to John Hancock's contacts in New Jersey.

25. This Court has personal jurisdiction over Defendant UBS because it has sufficient minimal contacts with this State in that it operates and engages in business in New Jersey, physical offices in New Jersey, and Plaintiffs' causes of action arise out of and relate to John Hancock's contacts in New Jersey.

26. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, DG3 is based in this District, DG3 maintains Plaintiffs' and Class Members' Private Information in this District pursuant to its client-vendor relationships with UBS and John Hancock requiring performance in this District, and Defendants have caused harm to Plaintiffs and Class Members in this District.

FACTUAL BACKGROUND

A. Defendants Owed Duties to Adopt Reasonable Data Security Measures for PII they Collected and Stored on their Systems.

27. Defendant John Hancock is an investment advisor firm providing portfolio management and related services to individual and institutional client customers across the United States.

28. Defendant UBS is a New-Jersey based financial services and insurance company.

29. Plaintiffs and Class Members are current and former customers of John Hancock and/or UBS.

30. As a condition of receiving services from John Hancock or UBS, John Hancock and UBS requires that its customers, including Plaintiffs and Class Members, entrust it with highly sensitive PII, including their names, addresses, contact information, Social Security numbers, and financial account information.

31. In exchange for receiving Plaintiffs' and Class Members' PII, John Hancock and UBS promised to safeguard the sensitive, confidential data and to only it for authorized and legitimate purposes, and to ensure the same practices from its vendors.

32. In the course of its client-vendor relationship with DG3, John Hancock and UBS provided the PII it collected from Plaintiffs and Class Members to DG3, and DG3 collected and maintained Plaintiffs' and Class Members' PII on its information technology systems and networks.

33. As a condition of obtaining services from DG3's clients, including John Hancock and UBS, Plaintiffs and Class Members were required to provide their sensitive and confidential PII to DG3 through John Hancock.

34. The information DG3 held in its computer networks at the time of the Data Breach

included the unencrypted PII of Plaintiffs and Class Members.

35. At all relevant times, Defendants knew DG3 was storing and using its networks to store and transmit valuable, sensitive PII belonging to Plaintiffs and Class Members, and that as a result, DG3's systems would be attractive targets for cybercriminals.

36. Defendants also knew that any breach of DG3's information technology network and exposure of the data stored therein would result in the increased risk of identity theft and fraud for the individuals whose PII was compromised, as well as intrusion into those individuals' highly private financial information.

37. Upon information and belief, Defendants made promises and representations to their customers, including Plaintiffs and Class Members, that the PII collected from them as a condition of directly and indirectly obtaining products and related services from Defendants would be kept safe and confidential, that the privacy of that information would be maintained, and that Defendants would delete any sensitive information after they were no longer required to maintain it and ensure their vendors did the same.

38. Indeed, John Hancock's Firm Brochure[5] assures that it has "established risk management systems reasonably designed to seek to reduce the risks associated with cyber-events," recognizing that "[a] cybersecurity breach could result in the loss or theft of customer data or funds[.]"[6] John Hancock further recognizes that "errors of [its] service providers" could cause a cybersecurity incident, like this Data Breach.[7]

---

[5] Available at https://files.adviserinfo.sec.gov/IAPD/Content/Common/crd_iapd_Brochure.aspx?BRCHR_VRSN_ID=903290 (last visited June 28, 2024).

[6] *Id.* at 18.

[7] *Id.*

39. DG3's Security and Data Policy, published on its website, touts, "Since its inception, DG3 has been constructed around the handling and producing of highly sensitive data for our clients. . . . DG3 is firmly obligated and committed to protect the confidentiality of this information."[8]

40. DG3's Data Handling and Privacy Agreement applicable to its client relationships, including with John Hancock, further warrants as follows[9]:

> DG3 and its DG3 Personnel will treat as confidential . . . all information and data which are proprietary to a third party (including but not limited to our client's customers and suppliers) and which our clients is obligated to treat as confidential, obtained by DG3 or its DG3 Personnel, or disclosed to DG3 or its DG3 Personnel in connection with the performance by DG3 of DG3's obligations under an agreement; and [] Customer Information (individually and collectively, "Confidential Information"). "Customer Information" means all information, in any form (e.g., written, verbal, electronic), provided to, or collected or generated by, the DG3 or to which the DG3 or its DG3 Personnel have been given access by or on behalf of our clients, that uniquely identifies a current, former or prospective our clients customer or customer of any correspondent bank or customer financial institution and includes, but is not limited to, Personal Information.
>
> * * *
>
> DG3 and its DG3 Personnel shall not disclose, use, publish or otherwise reveal, directly or indirectly through any third party, any Confidential Information (including without limitation Personal Information) to any third person or to any of DG3's DG3 Personnel that do not have a need to know such Confidential Information for the purpose of their role in performing DG3's obligations under an agreement. DG3 shall exercise the same degree of care to keep confidential any Confidential Information disclosed to DG3 as DG3 exercises to keep confidential its own information of like nature, but in no event less than a reasonable standard of care.

---

[8] *See* DG3 Data Security and Data Policy, https://dg3.com/data-and-security-policy/ (last visited June 28, 2024).

[9] *See* Data Handling and Privacy Agreement, https://dg3.com/data-and-security-policy/ (last visited June 28, 2024).

* * *

> DG3 will comply with data privacy laws in relation to the processing of personal data in connection with an agreement. DG3 will not, by any act or omission, place any member of our client's group in breach of the data privacy laws.

* * *

> DG3 will comply with, and only act on, instructions from and on behalf of the relevant member of the our [sic] client regarding the processing of our clients Personal Data and DG3 will not process the our [sic] clients Personal Data for any purposes other than to provide the Services to the relevant member of the our clients Group.

* * *

> DG3 will ensure that appropriate technical and organizational measures are taken to avoid unauthorized or unlawful processing of our clients Personal Data and against loss or destruction of or damage to our clients Personal Data.

* * *

> DG3 will inform the relevant member of the our clients immediately of any suspected or confirmed data protection breaches, unauthorized or unlawful processing, loss, or destruction of, or damage to, our clients Personal Data.

* * *

> DG3 will ensure that its DG3 Personnel are suitably informed, trained and instructed in respect of data privacy laws as well as obliged to observe data secrecy regulations pursuant to the relevant applicable data protection laws.

* * *

> DG3 will not, unless requested by our clients or obliged by law, disclose our clients Personal Data to any third party.

41. Plaintiffs and Class Members relied on these promises from Defendants, sophisticated business entities, to implement reasonable practices to keep their sensitive PII

confidential and securely maintained, to use this information for necessary purposes only and make only authorized disclosures of this information, and to delete PII from Defendants' systems when no longer necessary for its legitimate business purposes. But for Defendants' promises to keep Plaintiffs' and Class Members' PII secure and confidential, Plaintiffs and Class Members would not have transacted with or entrusted their PII to Defendants. Consumers, in general, demand security to safeguard their PII, especially when Social Security numbers and other sensitive financial information is involved.

42. But for Defendants' promises to keep Plaintiffs' and Class Members' PII secure and confidential, Plaintiffs and Class Members would not have transacted with or entrusted their PII to Defendants.

43. Based on the foregoing representations and warranties and to obtain services, directly and indirectly, from Defendants, Plaintiffs and Class Members provided their PII to Defendants with the reasonable expectation and on the mutual understanding that Defendants would comply with their promises and obligations to keep such information confidential and secure from unauthorized access.

44. Plaintiffs and Class Members value the confidentiality of their PII and demand security to safeguard their PII. To that end, Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII.

45. Defendants derived substantial economic benefits from collecting Plaintiffs' and Class Members' PII. Without the required submission of PII, Defendants could not perform the services they provide in the course of their business.

46. By obtaining, using, and benefitting from Plaintiffs' and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that they were

responsible for protecting Plaintiffs' and Class Members' PII from unauthorized access and disclosure.

47. Defendants had and have the duties to adopt reasonable measures to keep Plaintiffs' and Class Members' PII confidential and protected from involuntary disclosure to third parties, and to audit, monitor, and verify the integrity of their data management systems and those of their vendors and affiliates.

48. Additionally, Defendants had and have obligations created by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act"), the Gramm–Leach–Bliley Act, 15 U.S.C. § 6801(a) ("GLBA"), contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

B. Defendants Failed to Adequately Safeguard Plaintiffs' and Class Member's PII, resulting in the Data Breach.

49. On or about June 13, 2024, DG3 began sending Plaintiffs and other Data Breach victims the Notice Letter titled Notice of Data Breach.

50. The Notice Letters inform as follows:

> **What Happened?** On or around March 19, 2024, FG3 discovered suspicious activity on certain DG3 network systems and determined DG3 was experiencing a cyber incident. . . . Based on our investigation, we determined that certain information was accessed and/or copied from our systems between February 5th and 22nd, 2024. On or around April 26, 2024, we determined that information related to you was potentially impacted.
>
> **What Information Was Involved?** The types of information related to you that were affected by this incident include the following: name, address, email address, account number, and SSN.

51. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does

not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their PII remains protected.

52. Thus, DG3's "disclosure" amounts to no real disclosure at all, as it fails to inform Plaintiffs and Class Members of the Data Breach's critical facts with any degree of specificity. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

53. Because, according to DG3's Data Handling and Privacy Agreement, DG3 was required to notify John Hancock and UBS of the Data Breach within 24 hours of discovering it, on information and belief John Hancock and UBS learned of the Data Breach on or about March 19, 2024. Yet, John Hancock and UBS have failed to provide any independent notice of the Data Breach whatsoever to its customers whose PII was compromised, including Plaintiffs and Class Members.

54. As the Data Breach evidences, DG3 did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was collecting and maintaining for Plaintiffs and Class Members, such as encrypting the information or deleting it when it is no longer needed, and John Hancock and UBS failed to ensure its vendor used such reasonable security procedures and practices with respect to Plaintiffs' and Class Members' PII. These failures by Defendants caused the exposure and theft of Plaintiffs' and Class Members' PII in the Data Breach.

55. Plaintiffs' and Class Members' PII was accessed and stolen in the Data Breach. Criminal hackers accessed and acquired files stored without reasonable security on DG3's systems, which contained Plaintiffs' and Class Members' unencrypted PII.

56. Defendants could have prevented this Data Breach by properly securing and

encrypting the files and file servers containing Plaintiffs' and Class Members' PII, and ensuring the same from their vendors, but failed to do so.

57. Defendants' tortious conduct and breach of contractual obligations, as detailed herein, are evidenced by their failure to recognize the Data Breach until cybercriminals had already accessed Plaintiffs' and Class Members' PII, meaning Defendants had no effective means in place to ensure that cyberattacks were detected and prevented.

C. Defendants Knew or Should Have Known of the Risk of a Cyberattack because Companies in Possession of PII Are Particularly Suspectable.

58. Defendants' negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

59. At all relevant times, Defendants knew DG3 was using its network servers to store valuable, sensitive PII of UBS and John Hancock's customers, and that, as a result, these systems would be attractive targets for cybercriminals.

60. As custodians of Plaintiffs' and Class Members' PII, Defendants also knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiffs and Class Members, and of the foreseeable consequences if it or its vendor's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result.

61. Defendants also knew that any breach of DG3's systems, and exposure of the information stored therein would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised, as well as intrusion into their highly private financial information.

62. Data thieves regularly target companies like Defendants due to the highly sensitive information that they custody. Defendants knew and understood that unprotected PII is valuable

and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

63. PII of the kind accessed in the Data Breach is of great value to hackers and cybercriminals as it can be used for a variety of unlawful and nefarious purposes, including ransomware, fraudulent misuse, and sale on the Dark Web, due to the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[10]

64. As the Federal Trade Commission ("FTC") recognizes, identity thieves can use PII to commit an array of crimes including identity theft, and medical and financial fraud.[11] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and other protected financial information on multiple underground Internet websites on the Dark Web.

65. Criminals often trade stolen PII on the "cyber black market" for years following a breach. Cybercriminals can also post stolen PII on the internet, thereby making such information publicly available—indeed, that is precisely what happened with Plaintiffs' and Class Members' PII as a result of this Data Breach.

66. PII of the kind accessed in the Data Breach can also be used to distinguish, identify, or trace an individual's identity, such as his or her name, Social Security number, and financial records. This may be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as his or her birthdate, birthplace, and mother's maiden name.

---

[10] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

[11] *What To Know About Identity Theft*, FED. TRADE COMM'N CONSUMER ADVICE (Apr. 2021), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed Jan 23, 2024).

67. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting businesses that collect and store PII, like Defendants, preceding the date of this Data Breach.

68. These risks are not merely theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as CapitalOne, KeyBank, Equifax, Flagstar Bank, and TMX Finance Corporate Services, and many others.

69. Indeed, cyberattacks targeting businesses like Defendants are targeted and frequent. According to Contrast Security's 2023 report, "Cyber Bank Heists: Threats to the financial sector," "[o]ver the past year, attacks have included banking trojans, ransomware, account takeover, theft of client data and cybercrime cartels deploying 'trojanized' finance apps to deliver malware in spear-phishing campaigns."[12] In fact, "40% [of financial institutions] have been victimized by a ransomware attack."[13]

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

71. Additionally, as companies became more dependent on computer systems to run

[12] Contrast Security, "Cyber Bank Heists: Threats to the financial sector," pg. 5, avail. at https://www.contrastsecurity.com/hubfs/Cyber%20Bank%20Heists%20Report%2023.pdf?hsLang=en (last acc. February 9, 2024).

[13] *Id.*, at 15.

their business,[14] *e.g.*, working remotely as a result of the COVID-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[15]

72. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the United States.[16]

73. In tandem with the increase in data breaches, the rate of identity theft and the resulting losses has also increased over the past few years. For instance, in 2018, 14.4 million people were victims of some form of identity fraud, and 3.3 million people suffered unrecouped losses from identity theft, nearly three times as many as in 2016. And these out-of-pocket losses more than doubled from 2016 to $1.7 billion in 2018.[17]

74. According to the United States Government Accountability Office, which conducted a study regarding data breaches, "in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out

---

[14] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html (last visited Feb. 26, 2024).

[15] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (last visited Feb. 26, 2024).

[16] *Data Breach Report: 2021 Year End*, RISK BASED SECURITY (Feb. 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/.

[17] Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20(1).

all future harm."[18]

75. A poll of security executives predicted an increase in attacks over the next two years from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[19]

76. Due to high-profile data breaches at other businesses around the country, Defendants knew or should have known that DG3's information technology system would be targeted by cybercriminals.

77. Given the nature of the Data Breach, it was foreseeable that Plaintiffs' and Class Members' PII compromised therein would be targeted by hackers and cybercriminals for use in variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiffs' and Class Members' PII can easily obtain their tax returns or open fraudulent credit card accounts in Plaintiffs' and Class Members' names.

78. Defendants also knew or should have known the importance of safeguarding the PII with which they were entrusted and of the foreseeable consequences if their or their vendor's data security systems were breached. Defendants failed, however, to take adequate cybersecurity measures to detect or prevent the Data Breach and the exfiltration of Plaintiffs' and Class Members' PII from occurring.

79. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on DG3's server(s), namely, the detailed, sensitive PII of tens of

[18] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/assets/gao-07-737.pdf.

[19] Chuck Brooks, *Alarming Cyber Statistics For Mid-Year 2022 That You Need to Know*, FORBES (June 3, 2022), https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864.

thousands of individuals, if not more, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

80. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect Plaintiffs' and Class Members' PII from being compromised.

81. Plaintiffs and Class Members were the foreseeable and probable victims of Defendants' inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing PII and the critical importance of providing adequate security for that information.

82. The ramifications of Defendants' failure to keep Plaintiffs' and Class Members' PII secure are long lasting and severe. Once PII is stolen, the fraudulent use of that information and damage to victims may continue for years.

83. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for Plaintiffs' and Class Members' PII, including by failing to require reasonable data security measures in the course of Defendants' client-vendor relationship.

D. Defendants were Required, but Failed to Comply with FTC Guidelines.

84. Defendants are prohibited by section 5 of the FTC Act, 15 U.S.C. § 45, from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is "unfair practice" in violation of the FTC Act.

85. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need

for data security should be factored into all business decision-making.

86. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses like Defendants. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[20]

87. The FTC's guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[21]

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

89. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

90. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect third parties' confidential data, treating the failure to employ

[20] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION(2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed May 8, 2024).

[21] *Id.*

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 FTC Act. Orders resulting from these actions further clarify the measures business like Defendant must undertake to meet their data security obligations.

91. Such FTC enforcement actions include actions against entities like Defendants. *See, e.g., In the Matter of LabMD, Inc*., 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

92. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[22]

93. Defendants failed to properly implement one or more of the basic data security practices described above. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII resulted in the unauthorized access to and exfiltration of Plaintiffs' and Class Members' PII in the Data Breach.

94. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' PII or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

[22] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

E. Defendants were Required, but Failed, to Comply with the GLBA.

95. The Gramm–Leach–Bliley Act ("GLBA") states, "It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801(a).

96. Defendants are financial institutions for purposes of the GLBA, because they are "significantly engaged in financial activities, or significantly engaged in activities incidental to such financial activities." 16 C.F.R. § 314.2(h). Indeed, investment advisory companies like John Hancock are a specific example of financial institutions per GLBA-implemented regulations. *Id.* DG3 is a financial institution for purposes of the GLBA because it is significantly engaged in activities incidental to the financial services of its clients, including John Hancock. *Id.*

97. "Nonpublic personal information" means "personally identifiable financial information provided by a consumer to a financial institution; resulting from any transaction with the consumer or any service performed for the consumer; or otherwise obtained by the financial institution." 15 U.S.C. § 6809(4)(A)(i)–(iii).

98. The PII involved in the Data Breach constitutes "nonpublic personal information" for purposes of the GLBA.

99. Defendants collect "nonpublic personal information," as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) & 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period, Defendants were subject to the requirements of the GLBA, 15 U.S.C. §§ 6801, et seq., and to numerous rules and regulations promulgated under the GLBA.

100. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of

customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (i) designating one or more employees to coordinate the information security program; (ii) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (iii) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (iv) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (v) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 & 314.4. As alleged herein, Defendants violated the Safeguards Rule.

101. Defendants' conduct resulted in a variety of failures to follow GLBA-mandated rules and regulations, many of which are also industry standard. Among such deficient practices, the Data Breach demonstrates that Defendants (a) failed to implement (or inadequately implemented) information security policies or procedures such as effective employee training, sufficient intrusion detection systems, and regular reviews of audit logs and records; and (b) failed to oversee and require sufficient data security practices from service providers, to protect the confidentiality of the PII they collected and maintained in DG3's information technology systems.

102. Had Defendants implemented data security protocols, the consequences of the Data Breach could have been avoided, or at least significantly reduced as the Data Breach could have been detected earlier and the amount of PII compromised could have been greatly reduced.

F. Defendants Owed Plaintiffs and Class Members a Common Law Duty to Safeguard their PII.

103. In addition to their obligations under contract and federal law, Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants' duty owed to Plaintiffs and Class Members obligated them to provide, and ensure their vendors provided, reasonable data security, including consistency with industry standards and requirements, to ensure that their computer systems, networks, and protocols adequately protected Plaintiffs' and Class Members' PII.

104. Defendants owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the PII in DG3's possession, including ensuring that DG3 adequately trained its employees and others who accessed PII within DG3's computer systems on how to adequately protect such data.

105. Defendants owed a duty to Plaintiffs and Class Members to implement processes that would detect a compromise of PII in a timely manner.

106. Defendants owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

107. Defendants owed a duty to Plaintiffs and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

108. Defendants owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

109. Defendants tortiously failed to take the necessary precautions required to safeguard and protect Plaintiffs' and Class Members' PII from unauthorized disclosure. Defendants' actions

and omissions represent a flagrant disregard of Plaintiffs' and Class Members' rights.

G. Defendants Breached their Duties to Safeguard Plaintiffs' and Class Members' PII.

110. Defendants breached their obligations to Plaintiffs and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their servers, computer systems, and data and/or ensure their service providers did the same.

111. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

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

b. Failing to adequately protect customers' and/or their clients' customers' PII;

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

d. Failing to sufficiently train or require from their employees and vendors regarding the proper handling of customers' PII;

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

f. Failing to fully comply with the Safeguards Rule cybersecurity in violation of the GLBA;

g. Failing to provide timely or adequate notice to victims of the Data Breach; and

h. Otherwise breaching their duties and obligations to protect Plaintiffs' and Class Members' PII.

112. Defendants negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' PII by allowing cyberthieves to access DG3's servers and data management systems which contained unsecured and unencrypted PII.

113. Had Defendants remedied the deficiencies in their and/or their vendor's information storage and security systems, followed industry guidelines, and adopted security

measures recommended by experts in the field, they could and would have prevented intrusion into DG3's information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential PII.

H. Plaintiffs and Class Members Suffered Common Injuries and Damages due to Defendants' Conduct.

114. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including, without limitation, (a) invasion of privacy; (b) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) deprivation of value of their PII; and (g) the continued risk to their sensitive PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII they collect and maintain.

Increased Risk of Identity Theft

115. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[23] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien

[23] 17 C.F.R. § 248.201 (2013).

registration number, government passport number, employer or taxpayer identification number."[24]

116. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice:

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.[25]

117. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come because of the Data Breach.

118. The unencrypted PII of Plaintiffs and Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the Plaintiffs' and Class Members' PII.

119. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members.

120. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the

---

[24] *Id.*

[25] Erika Harrell, *Bureau of Just. Stat.*, U.S. DEP'T OF JUST., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed Jan. 23, 2024).

information to commit a variety of identity theft related crimes discussed below.

121. Social Security numbers, for example, allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often social security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes social security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

122. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

123. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

124. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information

through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

125. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[26]

126. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

127. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still 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.

128. The existence and prevalence of "Fullz" packages means that the PII stolen from

[26] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/ medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm (last visited Feb. 26, 2024).

the Data Breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiffs and the other Class Members.

129. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

130. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss Of Time to Mitigate Risk of Identity Theft and Fraud

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

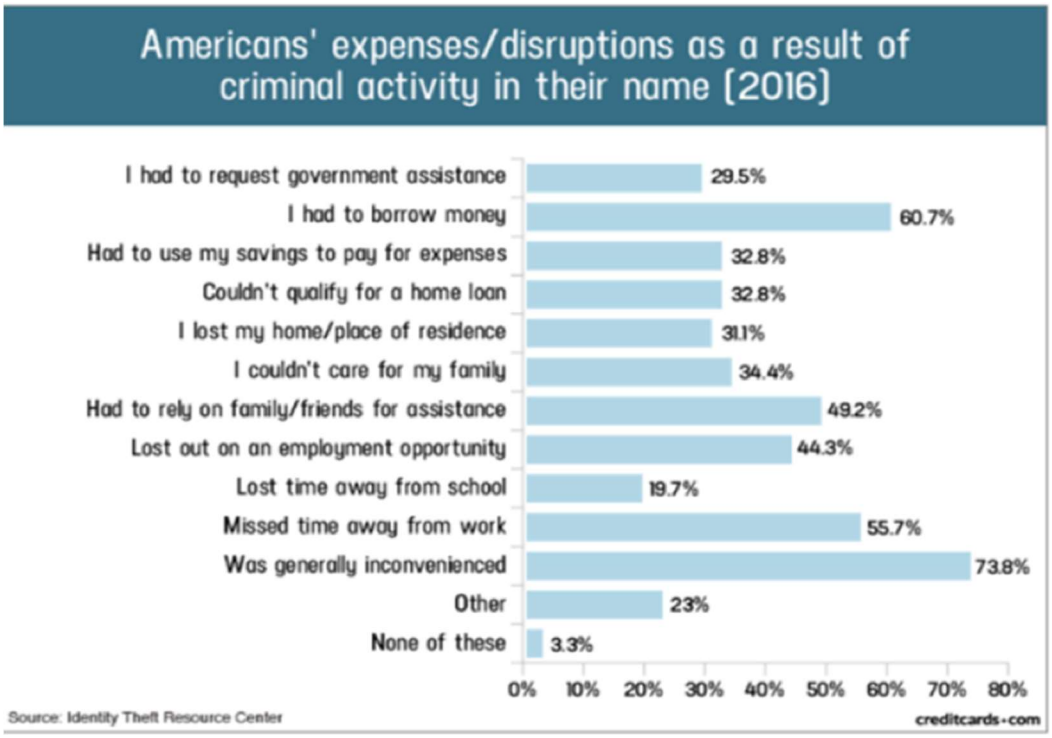
132. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must monitor their financial accounts for many years to mitigate that risk.

133. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and resecuring their own computer networks; and checking their financial accounts for any indication of fraudulent activity, which may take years to detect.

134. These efforts are consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud

alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[27]

135. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[28]



136. For those Class Members who experience actual identity theft and fraud, the GAO released a report in 2007 regarding data breaches, in which it noted that victims of identity theft

[27] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited Feb. 26, 2024).

[28] Jason Steele, "Credit Card and ID Theft Statistics," Oct. 24, 2017, https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Feb. 26, 2024).

will face "substantial costs and time to repair the damage to their good name and credit record."[29]

Diminution Value Of PII

137. PII is a valuable property right.[30] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

138. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[31]

139. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[32,33]

140. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[34] Conversely, sensitive PII can sell for as much as

---

[29] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," at 2, U.S. GOV'T ACCOUNTABILITY OFFICE, June 2007, https://www.gao.gov/ new.items/d07737.pdf (last visited Feb. 26, 2024) ("GAO Report").

[30] *See, e.g.*, Randall T. Soma, et al., Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[31] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Feb. 26, 2024).

[32] https://datacoup.com/ (last visited Feb. 26, 2024).

[33] https://digi.me/what-is-digime/ (last visited Feb. 26, 2024).

[34] Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Feb. 26, 2024).

$363 per record on the dark web according to the Infosec Institute.[35]

141. PII demands an even higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[36]

142. For example, PII can be sold at a price ranging from $40 to $200.[37] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[38]

143. Thus, Plaintiffs' and Class Members' compromised PII remains of high value to criminals, as evidenced by the prices they will pay through the Dark Web. Numerous sources cite dark web pricing for stolen identity credentials.[39]

144. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change, *e.g.*, names, identifying documents, dates of birth, and Social Security numbers.

---

[35] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Feb. 26, 2024).

[36] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Feb. 26, 2024).

[37] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN, Dec. 6, 2017, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Feb. 26, 2024).

[38] *In the Dark*, VPNOVERVIEW, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Feb. 26, 2024).

[39] *Your personal data is for sale on the dark web. Here's how much it costs,* DIGITAL TRENDS, Oct. 16, 2019, https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Feb. 26, 2024).

145. To illustrate, Social Security numbers—unlike credit or debit card numbers in a payment card data breach, which can quickly be frozen and reissued in the aftermath of a breach—cannot be easily replaced. Even when Social Security numbers are replaced, the process of doing so results in a major inconvenience to the subject individual, requiring a wholesale review of his or her relationships with government agencies and any number of private companies in order to update the individual's accounts with those entities.

146. The Social Security Administration even warns that the process of replacing a Social Security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[40]

147. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any

[40] Social Security Administration, *Identity Theft and Your Social Security Number*, July 2021, available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed April 30, 2024).

consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

148. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

Future Cost of Credit and Identity Theft Monitoring

149. The entire batch of Plaintiffs' and Class Members' stolen PII has already been placed on the Dark Web for any person with nefarious intentions to access, giving rise to a near-certainty that it will be further sold and purchased by criminals intending to utilize the PII for identity theft crimes—*e.g.,* opening bank accounts in the victims' names to make purchases or launder money; filing false tax returns; taking out loans or lines of credit; or filing false unemployment claims.

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

151. Consequently, Plaintiffs and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

152. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Plaintiffs and Class Members from the risk of identity theft that arose from the Data Breach caused

by Defendants' deficient data security processes. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendants' failure to safeguard their PII.

Loss of the Benefit of the Bargain

153. Furthermore, Defendants' poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to compensate and provide their PII to DG3's clients, including John Hancock and UBS, Plaintiffs and Class Members understood and expected that they were in part paying for Defendants' reasonable implementation and maintenance of reasonable data security measures to protect their confidential PII from unauthorized access and exposure, when in fact, Defendants did not provide the expected data security.

154. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with DG3's clients, namely, John Hancock and UBS.

Plaintiff Daniel Cunningham's Experience

155. At all times material hereto, Plaintiff is and was a customer of John Hancock, which provided investment advisement and portfolio management services to Plaintiff in exchange for Plaintiff's payment.

156. In the course and as a condition of receiving investment advisement and portfolio management services from John Hancock, Plaintiff was required to supply John Hancock with his PII—including, but not limited to his full name, date of birth, address, contact information, Social Security number, financial account information, and other sensitive information.

157. In the course and as a condition of receiving investment advisement and portfolio

management services from DG3's clients, including John Hancock, Plaintiff was required to supply DG3 with his PII. Pursuant to DG3 and John Hancock's vendor-client relationship, John Hancock provided the PII it collected from Plaintiff to DG3, and DG3 maintained and stored Plaintiff's PII on its computer network systems.

158. Plaintiff greatly values his privacy and is very careful about sharing his sensitive PII. Plaintiff diligently protects his PII and stores any documents containing PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

159. Plaintiff would not have entrusted his PII to Defendants had he known of Defendants' lax data security policies or that his PII would be maintained using inadequate data security systems that left it vulnerable to a cyberattack.

160. At the time of the Data Breach—in or around February 2024—Defendants retained Plaintiff's PII in their computer networks, which allowed Plaintiff's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

161. On or about June 13, 2024, Plaintiff received a written notification sent on DG3's behalf ("Notice Letter")[41] informing that his PII was accessed or exposed to unknown, unauthorized third parties through the Data Breach. According to the Notice Letter, unauthorized, unknown actors gained access to DG3's computer network systems between February 5 and February 22, 2024, and acquired files containing Plaintiff's sensitive PII, including his full name, address, email address, financial account number, and Social Security number.

162. The Notice Letter further informed Plaintiff that his PII in DG3's custody at the time of the Data Breach was provided to DG3 by John Hancock in the course of DG3 and John

[41] *See* Notice of Data Breach dated June 13, 2024, attached as **Exhibit "A"** hereto.

Hancock's vendor-client relationship.

163. In response to the Data Breach and the Notice Letter, Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff monitors his financial and credit statements multiple times a week and has already spent many hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

164. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

165. Plaintiff further believes his PII, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type. Moreover, following the Data Breach, Plaintiff has experienced suspicious spam and believes this be an attempt to secure additional PII from him.

166. The risk of identity theft is not speculative or hypothetical, but is impending and has materialized, as there is evidence that Plaintiff and Class Members' PII was targeted, accessed, misused, and disseminated on the Dark Web.

167. Other than the Data Breach, Plaintiff is not aware of ever being part of a data breach or similar cybersecurity incident involving his PII and is concerned that it has now been exposed to bad actors.

168. Subsequent to the Data Breach, Plaintiff has suffered numerous, substantial injuries including, but not limited to: (a) financial costs incurred mitigating the materialized risk and

imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) deprivation of value of his PII; (f) invasion of privacy; and (g) the continued risk to his sensitive PII, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect the PII they collect and maintain.

169. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence or the information stolen.

Plaintiff Debra De Salvo's Experience

170. Plaintiff Debra De Salvo is a customer of UBS, which, upon information and belief, contracts with Defendant DG3 for services.

171. As a condition of obtaining services at UBS, she was required to provide her PII to Defendant DG3, including her name, date of birth, address, and other sensitive information.

172. At the time of the Data Breach—February 5, 2024 through February 22, 2024--Defendant DG3 maintained Plaintiff's PII in its system.

173. Plaintiff De Salvo is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted her PII to Defendant DG3 had she known of Defendant DG3's lax data security policies.

174. Plaintiff Debra De Salvo received the Notice Letter, by U.S. mail, directly from

Defendant DG3, dated July 2, 2024.[42] According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including her name, address, at least one UBS account number, and date of birth.

175. As a result of the Data Breach, and at the direction of Defendant DG3's Notice Letter, which instructs Plaintiff to "remain vigilant to the possibility of unauthorized activity in your account(s)[,]"[43] Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach and monitoring her financial accounts for unusual activity. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

176. Plaintiff suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant DG3's possession and is subject to further unauthorized disclosures so long as Defendant DG3 fails to undertake appropriate and adequate measures to protect the PII.

177. Plaintiff further suffered actual injury in the form of her PII being disseminated on

[42] *See* Notice of Data Breach dated July 2, 2024, attached as **Exhibit "B"** hereto.

[43] Notice Letter.

the dark web, according to Experian, which, upon information and belief, was caused by the Data Breach.

178. Plaintiff additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of her PII was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

179. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant DG3 has still not fully informed her of key details about the Data Breach's occurrence.

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

181. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

182. Plaintiff Debra De Salvo has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant DG3's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

183. Plaintiffs bring this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following class:

Nationwide Class
All individuals residing in the United States whose PII was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Defendant in July 2024 (the "Class").

184. Plaintiff De Salvo additionally proposes the following class definition, subject to amendment as appropriate:

Illinois Subclass
All individuals residing in the State of Illinois whose PII was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Defendant in July 2024 (the "Illinois Subclass").

185. Excluded from the Classes are Defendants, their subsidiaries and affiliates, their officers, directors and members of their immediate families, and any entity in which Defendants have a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

186. Plaintiffs reserve the right to modify or amend the definition of the proposed Classes prior to moving for class certification.

187. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation, and membership in the proposed classes is easily ascertainable.

188. **Numerosity:** The Class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendants' records, including but not limited to, the files implicated in the Data Breach. Upon information and belief, the Class includes at least tens of thousands of individuals.

189. **Commonality:** This action involves questions of law and fact that are common to all Class Members. Such common questions include, but are not limited to the following:

a. Whether Defendants had a duty to protect the PII of Plaintiffs and Class Members;

b. Whether Defendants were negligent in collecting and storing Plaintiffs' and Class Members' PII, and breached their duties thereby;

c. Whether Defendant John Hancock was negligent in overseeing its vendors and ensuring they implemented reasonable data security measures for Plaintiffs' and Class Members' PII;

d. Whether Defendants breached implied contracts with Plaintiffs and Class Members to use reasonable means to protect their PII;

e. Whether Defendants breached third-party beneficiary contracts to use reasonable means to protect Plaintiffs' and Class Members' PII;

f. Whether Defendants breached their fiduciary duties to Plaintiffs and Class Members;

g. Whether Defendants were unjustly enriched by failing to implement reasonable or adequate data security measures for Plaintiffs' and Class Members' PII;

h. Whether Plaintiffs and Class Members are entitled to damages as a result of Defendants' wrongful conduct;

i. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

j. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

190. **Typicality:** Plaintiffs' claims are typical of the claims of the Class Members. The claims of the Plaintiffs and members of the Class are based on the same legal theories and arise from the same failure by Defendants to safeguard PII. Plaintiffs and Class Members all provided their PII to Defendants and had their PII accessed, exfiltrated, and compromised in the Data Breach.

191. **Adequacy of Representation:** Plaintiffs is an adequate representative of the Class because his interests do not conflict with the interests of the other Class Members Plaintiffs seek to represent; Plaintiffs has retained counsel competent and experienced in complex class action litigation, specifically litigation involving data breaches; Plaintiffs intend to prosecute this action vigorously; and Plaintiffs' counsel have adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiffs and Plaintiffs' counsel.

192. **Predominance.** Common questions of law and fact predominate over any questions affecting only individual Class Members. For example, Defendant's liability and the fact of damages is common to Plaintiffs and each member of the Classes. If Defendant breached its common law and statutory duties to secure Private Information on its network server, then Plaintiffs and each Class Member suffered damages from the exposure of sensitive Private Information in the Data Breach.

193. **Superiority.** Given the relatively low amount recoverable by each Class Member, the expenses of individual litigation are insufficient to support or justify individual suits, making this action superior to individual actions.

194. **Manageability.** The precise size of the Classes is unknown without the disclosure of Defendant's records. The claims of Plaintiffs and the Class Members are substantially identical as explained above. Certifying the case as a class action will centralize these substantially identical claims in a single proceeding and adjudicating these substantially identical claims at one time is the most manageable litigation method available to Plaintiffs and the Classes.

FIRST CAUSE OF ACTION
NEGLIGENCE/NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class against Defendants)

195. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 194 above as if fully set forth herein.

196. Defendants gathered and stored the PII of Plaintiffs and Class Members in the course and scope of their respective businesses.

197. Plaintiffs and Class Members entrusted Defendants with their PII with the understanding that Defendants would safeguard that sensitive information.

198. Defendants' duty to use reasonable care arose from several sources, including but not limited to those described below.

199. Defendants owed a duty under common law to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiffs and Class Members' PII in Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

200. Defendants owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their and their vendors' systems and networks, and the personnel responsible for them, adequately protected the PII.

201. Defendants had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

202. By assuming the responsibility to collect and store this data, and in fact doing so, and using it for commercial gain, Defendants had duties of care to use reasonable means to secure and to prevent disclosure of the information, to safeguard the information from theft, and to ensure

the same from their vendors and service providers. Defendants' duties included a responsibility to audit, monitor, and ensure the integrity of their systems and practices and to give prompt notice to those affected in the case of a data breach.

203. John Hancock's and UBS's duties of care to use, and ensure its service providers used, reasonable security measures further arose as a result of the special relationship that existed between John Hancock and UBS, on one hand, and Plaintiffs and Class Members, on the other. That special relationship arose because Plaintiffs and the Class entrusted Defendants with their confidential PII, a necessary part of obtaining services at John Hancock and UBS.

204. Moreover, Defendants had a duty to promptly and adequately notify Plaintiffs and Class Members of the Data Breach.

205. Defendants had and continue to have a duty to adequately disclose that the PII of Plaintiffs and Class Members within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice is and was necessary to allow Plaintiffs and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

206. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs or Class Members.

207. Defendants had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendants. By collecting and storing valuable PII that is routinely targeted by criminals for unauthorized access, Defendants were obligated to act with reasonable care to protect against these foreseeable threats.

208. Defendants' duties also arose from their position as sophisticated businesses and

employers. Defendants hold themselves out as a trusted and legally compliant enterprise, and thereby assume a duty to reasonably protect their customers' information. Indeed, as sophisticated business entities, Defendants were in a unique and superior position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

209. Defendants breached the duties owed to Plaintiffs and Class Members and thus were negligent. Defendants breached these duties by, among other things: (a) mismanaging their systems and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling their data security by failing to assess the sufficiency of their safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust their information security program in light of the circumstances alleged herein; (f) failing to adequately oversee their vendors to ensure they had reasonable and adequate data security measurements in place to protect individuals' PII; (g) failing to detect the Data Breach at the time it began or within a reasonable time thereafter; (h) failing to notify about the Data Breach within a reasonable time after it was discovered; and (i) failing to follow their own privacy policies and practices that they published.

210. But for Defendants' wrongful and negligent breaches of their duties owed to Plaintiffs and Class Members, Plaintiffs' and Class Members' PII would not have been compromised in the Data Breach, and their resulting injuries would not have occurred.

211. Further, 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 entities

such as Defendants of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendants' duties.

212. Defendants violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiffs' and Class Members' PII and not complying with the industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII they collected, obtained, shared, and stored and the foreseeable consequences of a data breach involving the PII of their or their clients' customers.

213. Plaintiffs and members of the Class are consumers within the class of persons Section 5 of the FTCA was intended to protect.

214. The harm that has occurred as a result of Defendants' conduct is the type of harm that the FTCA was intended to guard against.

215. Defendants' violations of Section 5 of the FTCA constitute negligence *per se*.

216. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

217. Defendants violated Section 501(b) of the GLBA and the Safeguards Rule by failing to implement and/or inadequately implementing information security policies or procedures such as effective employee training, adequate intrusion detection systems, regular reviews of audit logs and records, and other similar measures to protect the confidentiality of Plaintiffs' and Class Members' PII, and/or by failing to oversee their service providers to ensure these data security measures were being implemented.

218. Plaintiffs and members of the Class are consumers within the class of persons

Section 501(b) of the GLBA and the Safeguards Rule were intended to protect.

219. The harm that has occurred as a result of Defendants' conduct is the type of harm that Section 501(b) of the GLBA and the Safeguards Rule were intended to guard against.

220. Defendants' violations of Section 501(b) of the GLBA and the Safeguards Rule constitute negligence *per se*.

221. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have suffered injuries, including without limitation the following:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of PII;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores due to from credit inquiries for fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

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

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs' and Class Members' PII against theft and not allow access and misuse of their data by others; and

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data.

222. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class

Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff Cunningham and the Class against Defendant John Hancock)

223. Plaintiff Cunningham ("Plaintiff" for the purposes of this count) re-alleges and incorporates by reference paragraphs 1 through 194 above as if fully set forth herein.

224. Plaintiff and Class Members were required to provide their PII to John Hancock as a condition of receiving products and related services from John Hancock, and did in fact entrust their PII to John Hancock in exchange for receiving such products and services.

225. When Plaintiff and Class Members provided their PII to John Hancock in exchange for receiving investment management products and/or services from John Hancock, they entered into implied contracts with John Hancock under which John Hancock agreed to take reasonable steps to safeguard and protect Plaintiff's and Class Members' PII, to keep such information secure and confidential, to ensure its vendors, including DG3, implemented reasonable steps to safeguard and protect Plaintiff's and Class Members' PII and keep that data confidential, and to timely and accurately notify Plaintiff and Class Members if their PII had been compromised or stolen in a cybersecurity incident like the Data Breach.

226. Implicit in the implied contractual agreement between Plaintiff and Class Members and John Hancock were John Hancock's promises and obligations to (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect Plaintiff's and Class Members' PII from unauthorized disclosure or uses, (f) retain the PII only under

conditions that kept such information secure and confidential, and (e) ensure its vendors, including DG3, used the foregoing measures with respect to Plaintiff's and Class Members' PII that John Hancock provided it.

227. In entering into such implied contracts with John Hancock, Plaintiff and Class Members reasonably believed and expected that John Hancock's data security practices complied with applicable laws and regulations and were consistent with industry standards.

228. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and John Hancock, on the other, is demonstrated by their conduct and course of dealing.

229. John Hancock solicited, offered, and invited Plaintiff and Class Members to provide their PII as part of John Hancock's regular business practices. Plaintiff and Class Members accepted John Hancock's offers and provided their PII to John Hancock.

230. In accepting the PII of Plaintiff and Class Members, John Hancock understood and agreed that it was required to reasonably safeguard the PII from unauthorized access or disclosure, including by ensuring reasonable and adequate data security measures from its vendors, including DG3.

231. On information and belief, at all relevant times John Hancock promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose their PII under certain circumstances, none of which relate to the Data Breach.

232. John Hancock's promises to safeguard Plaintiff's and Class Members' PII is evidenced by, for example, the representations in John Hancock's brochure as set forth above.

233. On information and belief, John Hancock further promised to provide Plaintiff's and Class Members' PII to vendors that complied with industry standards to make sure that

Plaintiff's and Class Members' PII would remain protected.

234. Plaintiff and Class Members provided their PII to John Hancock with the reasonable belief and expectation that John Hancock would use part of its earnings to obtain adequate data security for their PII. John Hancock failed to do so.

235. Plaintiff and Class Members would not have entrusted their PII to John Hancock in the absence of the implied contract between them and John Hancock obligating John Hancock to keep Plaintiff's and Class Members' PII reasonably secure.

236. Plaintiff and Class Members would not have entrusted their PII to John Hancock in the absence of John Hancock's implied promise to ensure that it and its vendors, including DG3, adopted reasonable data security measures.

237. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with John Hancock, including by providing their PII to John Hancock.

238. John Hancock breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their PII, failing to delete Plaintiff's and Class Members' PII once the relationship ended, failing to provide timely or adequate notice to Plaintiff and Class Members that their PII was compromised as a result of the Data Breach, and failing to ensure the same from its vendors, including DG3.

239. As a direct and proximate result of John Hancock's breach of its implied contracts with Plaintiff and Class Members, Plaintiff and Class Members sustained damages as alleged herein, including the loss of the benefit of their bargain.

240. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered due to John Hancock's breach of implied contract and the resulting Data Breach.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff Cunningham and the Class against Defendant UBS)

241. Plaintiff De Salvo ("Plaintiff" for the purposes of this count) re-alleges and incorporates by reference paragraphs 1 through 194 above as if fully set forth herein.

242. Plaintiff and Class Members were required to provide their PII to UBS as a condition of receiving products and related services from UBS, and did in fact entrust their PII to UBS in exchange for receiving such products and services.

243. When Plaintiff and Class Members provided their PII to UBS in exchange for receiving products and/or services from UBS, they entered into implied contracts with UBS under which UBS agreed to take reasonable steps to safeguard and protect Plaintiff's and Class Members' PII, to keep such information secure and confidential, to ensure its vendors, including DG3, implemented reasonable steps to safeguard and protect Plaintiff's and Class Members' PII and keep that data confidential, and to timely and accurately notify Plaintiff and Class Members if their PII had been compromised or stolen in a cybersecurity incident like the Data Breach.

244. Implicit in the implied contractual agreement between Plaintiff and Class Members and UBS were UBS's promises and obligations to (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect Plaintiff's and Class Members' PII from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential, and (e) ensure its vendors, including DG3, used the foregoing measures with respect to Plaintiff's and Class Members' PII that UBS provided it.

245. In entering into such implied contracts with UBS, Plaintiff and Class Members

reasonably believed and expected that UBS's data security practices complied with applicable laws and regulations and were consistent with industry standards.

246. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and UBS, on the other, is demonstrated by their conduct and course of dealing.

247. UBS solicited, offered, and invited Plaintiff and Class Members to provide their PII as part of UBS's regular business practices. Plaintiff and Class Members accepted UBS's offers and provided their PII to UBS.

248. In accepting the PII of Plaintiff and Class Members, UBS understood and agreed that it was required to reasonably safeguard the PII from unauthorized access or disclosure, including by ensuring reasonable and adequate data security measures from its vendors, including DG3.

249. On information and belief, at all relevant times UBS promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose their PII under certain circumstances, none of which relate to the Data Breach.

250. UBS's promises to safeguard Plaintiff's and Class Members' PII is evidenced by, for example, the representations in UBS's brochure as set forth above.

251. On information and belief, UBS further promised to provide Plaintiff's and Class Members' PII to vendors that complied with industry standards to make sure that Plaintiff's and Class Members' PII would remain protected.

252. Plaintiff and Class Members provided their PII to UBS with the reasonable belief and expectation that UBS would use part of its earnings to obtain adequate data security for their PII. UBS failed to do so.

253. Plaintiff and Class Members would not have entrusted their PII to UBS in the absence of the implied contract between them and UBS obligating UBS to keep Plaintiff's and Class Members' PII reasonably secure.

254. Plaintiff and Class Members would not have entrusted their PII to UBS in the absence of UBS's implied promise to ensure that it and its vendors, including DG3, adopted reasonable data security measures.

255. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with UBS, including by providing their PII to UBS.

256. UBS breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their PII, failing to delete Plaintiff's and Class Members' PII once the relationship ended, failing to provide timely or adequate notice to Plaintiff and Class Members that their PII was compromised as a result of the Data Breach, and failing to ensure the same from its vendors, including DG3.

257. As a direct and proximate result of UBS's breach of its implied contracts with Plaintiff and Class Members, Plaintiff and Class Members sustained damages as alleged herein, including the loss of the benefit of their bargain.

258. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered due to UBS's breach of implied contract and the resulting Data Breach.

FOURTH CAUSE OF ACTION
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiffs and the Class against DG3)

259. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 194 above as if fully set forth herein.

260. Upon information and belief, DG3 entered into virtually identical contracts with its

clients, including John Hancock and UBS, to provide marketing and related services, which included data security practices, procedures, and protocols sufficient to safeguard the PII that was to be entrusted to it.

261. Such contracts were made expressly for the benefit of Plaintiffs and Class Members, as it was their PII that DG3 agreed to receive and protect through its services.

262. Thus, the benefit of collection and protection of the PII belonging to Plaintiffs and Class Members was the direct and primary objective of the contracting parties, and Plaintiffs and Class Members were direct and express beneficiaries of such contracts.

263. DG3 knew that if they were to breach these contracts with its clients, Plaintiffs and Class Members would be harmed and suffer consequential damages.

264. DG3 breached its contracts with its clients and, as a result, Plaintiffs and Class Members were affected by this Data Breach when DG3 failed to use reasonable data security monitoring and prevention measures that could and would have prevented the Data Breach and Plaintiffs and Class Members' resulting injuries and damages.

265. As foreseen, Plaintiffs and Class Members were harmed by DG3's failure to use reasonable data security measures to securely store and protect their PII in its custody and care, including but not limited to, the continuous and substantial risk of harm through the loss of their PII.

266. As a direct and proximate result of John Hancock's breach of its implied contracts with Plaintiffs and Class Members, Plaintiffs and Class Members sustained damages as alleged herein.

267. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered due to DG3's breach of third-party beneficiary contracts and the

resulting Data Breach and injuries it caused to Plaintiffs and Class Members.

FIFTH CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff Cunningham and the Class against John Hancock)

268. Plaintiff Cunningham ("Plaintiff" for the purposes of this count) re-allege and incorporate by reference paragraphs 1 through 194 above as if fully set forth herein.

269. Plaintiff and Class Members have an interest, both equitable and legal, in the PII about them that was conveyed to, collected by, and shared to vendors by John Hancock and that was ultimately accessed or compromised in the Data Breach.

270. As a financial institution and investment advisor, John Hancock has a fiduciary relationship with their customers, including Plaintiff and the Class Members.

271. Because of that fiduciary relationship, John Hancock was provided with, stored, and allowed its vendors to store private and valuable PII related to Plaintiff and Class Members, which John Hancock was required to maintain in confidence and ensure its vendors did the same.

272. John Hancock owed fiduciary duties under common law to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiff's and Class Members' PII in John Hancock's possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

273. As a result of the parties' fiduciary relationship, John Hancock had an obligation to maintain the confidentiality of Plaintiff's and the Class Members' PII stored in its vendors' systems.

274. Customers like Plaintiff and Class Members have a privacy interest in personal financial matters, and John Hancock had a fiduciary duty not to disclose financial data concerning its customers.

275. As a result of the parties' relationship, John Hancock had possession and knowledge of confidential PII of Plaintiff and Class Members, information not generally known.

276. Plaintiff and Class Members did not consent to nor authorize John Hancock to release or disclose their PII to vendors or service providers that failed to implement and maintain reasonable or adequate data security practices.

277. John Hancock breached the duties owed to Plaintiff and Class Members by, among other things: (a) failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII in the Data Breach; (b) mishandling its data security by failing to assess the sufficiency of its or its vendors', including DG3's, safeguards in place to control these risks; (c) failing to design and implement, or to ensure its vendors, including DG3, designed and implemented, information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to adequately oversee, evaluate, and require adjustment to their vendors', including DG3's, information security program in light of the circumstances alleged herein; (f) failing to detect the Data Breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its customers; (h) entrusting Plaintiff's and Class Members' PII to vendors, including DG3, that allowed an unauthorized and unjustified disclosure and release of Plaintiff and the Class Members' PII to a criminal third party; and (i) failing to provide timely or adequate notice to Plaintiff and Class Members about the Data Breach.

278. But for John Hancock's wrongful breach of its fiduciary duties owed to Plaintiff and Class Members, Plaintiff's and Class Members' privacy, confidences, and PII would not have been compromised.

279. As a direct and proximate result of John Hancock's breach of its fiduciary duties, Plaintiff and Class Members have suffered injuries, including without limitation the following:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of PII;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores due to from credit inquiries for fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

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

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to John Hancock with the mutual understanding that John Hancock would safeguard Plaintiff's and Class Members' PII against theft and not allow access and misuse of their data by others; and

h. Continued risk of exposure to hackers and thieves of their PII, which remains in John Hancock's and DG3's possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data.

280. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered due to John Hancock's breaches of fiduciary duty and the resulting Data Breach.

SIXTH CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff De Salvo and the Class against UBS)

281. Plaintiff De Salvo ("Plaintiff" for the purposes of this count) re-allege and incorporate by reference paragraphs 1 through 194 above as if fully set forth herein.

282. Plaintiff and Class Members have an interest, both equitable and legal, in the PII about them that was conveyed to, collected by, and shared to vendors by UBS and that was ultimately accessed or compromised in the Data Breach.

283. As a financial institution, UBS has a fiduciary relationship with their customers, including Plaintiff and the Class Members.

284. Because of that fiduciary relationship, UBS was provided with, stored, and allowed its vendors to store private and valuable PII related to Plaintiff and Class Members, which UBS was required to maintain in confidence and ensure its vendors did the same.

285. UBS owed fiduciary duties under common law to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiff's and Class Members' PII in UBS's possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

286. As a result of the parties' fiduciary relationship, UBS had an obligation to maintain the confidentiality of Plaintiff's and the Class Members' PII stored in its vendors' systems.

287. Customers like Plaintiff and Class Members have a privacy interest in personal financial matters, and UBS had a fiduciary duty not to disclose financial data concerning its customers.

288. As a result of the parties' relationship, UBS had possession and knowledge of confidential PII of Plaintiff and Class Members, information not generally known.

289. Plaintiff and Class Members did not consent to nor authorize UBS to release or disclose their PII to vendors or service providers that failed to implement and maintain reasonable or adequate data security practices.

290. UBS breached the duties owed to Plaintiff and Class Members by, among other

things: (a) failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII in the Data Breach; (b) mishandling its data security by failing to assess the sufficiency of its or its vendors', including DG3's, safeguards in place to control these risks; (c) failing to design and implement, or to ensure its vendors, including DG3, designed and implemented, information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to adequately oversee, evaluate, and require adjustment to their vendors', including DG3's, information security program in light of the circumstances alleged herein; (f) failing to detect the Data Breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its customers; (h) entrusting Plaintiff's and Class Members' PII to vendors, including DG3, that allowed an unauthorized and unjustified disclosure and release of Plaintiff and the Class Members' PII to a criminal third party; and (i) failing to provide timely or adequate notice to Plaintiff and Class Members about the Data Breach.

291. But for UBS's wrongful breach of its fiduciary duties owed to Plaintiff and Class Members, Plaintiff's and Class Members' privacy, confidences, and PII would not have been compromised.

292. As a direct and proximate result of UBS's breach of its fiduciary duties, Plaintiff and Class Members have suffered injuries, including without limitation the following:

i. Theft of their PII;

j. Costs associated with the detection and prevention of identity theft and unauthorized use of PII;

k. Costs associated with purchasing credit monitoring and identity theft protection services;

l. Lowered credit scores due to from credit inquiries for fraudulent activities;

m. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

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

o. Damages to and diminution in value of their PII entrusted, directly or indirectly, to UBS with the mutual understanding that UBS would safeguard Plaintiff's and Class Members' PII against theft and not allow access and misuse of their data by others; and

p. Continued risk of exposure to hackers and thieves of their PII, which remains in UBS's and DG3's possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data.

293. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered due to UBS's breaches of fiduciary duty and the resulting Data Breach.

SEVENTH CAUSE OF ACTION
BREACH OF CONFIDENCE
(On Behalf of Plaintiffs and the Class against Defendants)

294. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 194 above as if fully set forth herein.

295. Plaintiffs and Class Members have an interest, both equitable and legal, in the PII about them that was conveyed to, collected by, and maintained by Defendants and that was ultimately accessed or compromised in the Data Breach.

296. As businesses that collect and store the PII of their or their clients' customers, Defendants are in a position of trust and confidence *vis-à-vis* the individuals whose PII they collect and maintain, including Plaintiffs and Class Members, and have a special relationship with such

individuals.

297. Because of that special relationship, Defendants were provided with and stored private and valuable PII pertaining to Plaintiffs and Class Members, which Defendants were required to maintain in confidence.

298. Plaintiffs and the Class provided Defendants with their personal and confidential PII under both the express and/or implied agreement of Defendants to limit the use and disclosure of such PII through reasonable and adequate information security measures.

299. Defendants owed duties to Plaintiffs and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in Defendants' possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

300. Defendants had an obligation to maintain the confidentiality of Plaintiffs' and the Class Members' PII.

301. Plaintiffs and Class Members have a privacy interest in their personal financial matters, and Defendants had a duty not to disclose confidential financial information and records concerning their or their clients' customers.

302. As a result of the parties' relationship, Defendants had possession and knowledge of confidential PII and confidential personal financial data of Plaintiffs and Class Members.

303. Plaintiffs' and Class Members' PII is not generally known to the public and is confidential by nature.

304. Plaintiffs and Class Members did not consent to nor authorize Defendants to release or disclose their PII to an unknown criminal actor.

305. Defendants breached the duties of confidence owed to Plaintiffs and Class

Members when Plaintiffs' and Class's PII was disclosed to unknown criminal hackers.

306. Defendants breached their duties of confidence by failing to safeguard Plaintiffs' and Class Members' PII, including by, among other things: (a) mismanaging their system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling their data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust their information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow their own privacy policies and practices published to their customers; (h) storing PII in an unencrypted and vulnerable manner, allowing its disclosure to hackers; (i) making an unauthorized and unjustified disclosure and release of Plaintiffs and the Class Members' PII and financial records/information to a criminal third party; and (j) failing to prevent the foregoing from their vendors and/or service providers in possession of Plaintiffs' and Class Members' PII.

307. But for Defendants' wrongful breach of the duty of confidences owed to Plaintiffs and Class Members, Plaintiffs' and Class Members' privacy, confidences, and PII would not have been compromised.

308. As a direct and proximate result of Defendants' breach of Plaintiffs' and the Class's confidences, Plaintiffs and Class Members have suffered injuries, including:

a. The erosion of the essential and confidential relationship between Defendants and Plaintiffs and Class Members;

b. Loss of their privacy and confidentiality in their PII;

c. Theft of their PII;

d. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

e. Costs associated with purchasing credit monitoring and identity theft protection services;

f. Lowered credit scores resulting from credit inquiries following fraudulent activities;

g. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

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

i. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendants would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

j. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data;

k. Loss of personal time spent carefully reviewing statements and records to check for charges for services not received; and

l. Mental anguish accompanying the loss of confidences and disclosure of their confidential and private PII.

309. Additionally, Defendants received payments from Plaintiffs and Class Members, directly or indirectly, for products and services with the understanding that Defendants would uphold their responsibilities to maintain the confidence of Plaintiffs' and Class Members' PII.

310. Defendants breached the confidence of Plaintiffs and Class Members when they

failed to use reasonable or adequate data security measures to prevent the unauthorized release and disclosure of Plaintiffs' and Class Members' confidential PII in the Data Breach and, accordingly, it would be inequitable for Defendants to retain the benefit at Plaintiffs and Class Members' expense.

311. As a direct and proximate result of Defendants' breaches of Plaintiffs' and Class Members' confidence, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

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

312. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 194 above as if fully set forth herein.

313. This claim is pleaded in the alternative to the claim of breach of implied contract (Count III) and the claim of breach of third-party beneficiary contract (Count IV).

314. Plaintiffs and Class Members conferred direct benefits upon Defendants in the form of agreeing to provide their PII to Defendants, directly or indirectly, without which Defendants could not perform the services they provide or operate their business.

315. Defendants appreciated or knew of these benefits they received from Plaintiffs and Class Members. Under principles of equity and good conscience, Defendants should not be allowed to retain the full value of these benefits—specifically, the costs they saved by failing to implement reasonable or adequate data security practices with respect to the PII they collected, directly and indirectly, from Plaintiffs and Class Members.

316. After all, Defendants failed to adequately protect Plaintiffs' and Class Members'

PII. If such data security inadequacies were known, Plaintiffs and Class Members would never have agreed to provide their PII or payment, to Defendants.

317. Defendants should be compelled to disgorge into a common fund, for the benefit of Plaintiffs and the Class, all funds that were unlawfully or inequitably gained despite Defendants' misconduct and the resulting Data Breach.

NINTH CAUSE OF ACTION
VIOLATION OF THE ILLINOIS CONSUMER FRAUD ACT
815 Ill. Comp. Stat. §§ 505/1, *et seq.*
(On Behalf of Plaintiff De Salvo and the Illinois Subclass against Defendants DG3 and UBS)

318. Plaintiff De Salvo ("Plaintiff" for the purposes of this count) re-alleges and incorporates by reference paragraphs 1 through 194 above as if fully set forth herein, as if fully set forth herein, and brings this claim on behalf of herself and the Illinois Subclass (the "Class" for the purposes of this count) against Defendants DG3 and UBS ("Defendants" for the purposes of this count).

319. Plaintiff and the Class are "consumers" as that term is defined in 815 ILL. COMP. STAT. § 505/1(e).

320. Plaintiff, the Class, and Defendants are "persons" as that term is defined in 815 ILL. COMP. STAT. § 505/1(c).

321. Defendants are engaged in "trade" or "commerce," including the provision of services, as those terms are defined under 815 ILL. COMP. STAT. § 505/1(f).

322. Defendants engage in the "sale" of "merchandise" (including services) as defined by 815 ILL. COMP. STAT. § 505/1(b) and (d).

323. Defendants' acts, practices, and omissions were done in the course of Defendants' business of marketing, offering for sale, and selling services in the State of Illinois.

324. Defendants engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in connection with the sale and advertisement of "merchandise" (as defined in the Illinois CFA) in violation of the Illinois CFA, including, but not limited to, the following:

a. failure to maintain adequate computer systems and data security practices to safeguard its clients' current and former customers' PII;

b. failure to disclose the material fact that its computer systems and data security practices were inadequate to safeguard the personal information it was collecting and maintaining from theft;

c. failure to disclose in a timely and accurate manner to Plaintiff and the Class Members the material fact of Defendants' data breach;

d. misrepresenting material facts to Plaintiff and the Class, in connection with the sale of goods and services, by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Class members' PII from unauthorized disclosure, release, data breaches, and theft;

e. misrepresenting material facts to the class, in connection with the sale of goods and services, by representing that Defendants did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff's and Class members' PII, and

f. failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff's and Class members' PII from further unauthorized disclosure, release, data breaches, and theft.

325. In addition, Defendants' failure to disclose that its computer systems were not well

protected and that Plaintiff's and Class members' sensitive information was vulnerable and susceptible to intrusion and cyberattacks constitutes deceptive and/or unfair acts or practices because Defendants knew such facts would (a) be unknown to and not easily discoverable by Plaintiff and the Class; and (b) defeat Plaintiff's and Class members' ordinary, foreseeable and reasonable expectations concerning the security of their PII on Defendants' servers.

326. Defendants intended that Plaintiff and the Class rely on its deceptive and unfair acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts, in connection with Defendants' offering of goods and services and storing Plaintiff's and Class members' PII on its servers, in violation of the Illinois CFA.

327. Defendants also engaged in unfair acts and practices by failing to maintain the privacy and security of class members' personal information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach.

328. These unfair acts and practices violated duties imposed by laws including Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45) and similar state laws.

329. Defendants' wrongful practices occurred in the course of trade or commerce.

330. Defendants' wrongful practices were and are injurious to the public interest because those practices were part of a generalized course of conduct on the part of Defendants that applied to all Class members and were repeated continuously before and after Defendants obtained PII from Plaintiff and Class members.

331. All Class members have been adversely affected by Defendants conduct and the public was and is at risk as a result thereof.

332. As a direct and proximate result of Defendants' conduct, Plaintiff and Class members have suffered harm, including, but not limited to: (i) invasion of privacy; (ii) theft of

their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiff's PII being disseminated on the dark web, according to Experian; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the PII.

333. Pursuant to 815 ILL. COMP. STAT. § 505/10a(a), Plaintiff seeks actual, compensatory, and punitive damages (pursuant to 815 ILL. COMP. STAT. § 505/10a(c)), injunctive relief, and court costs and attorneys' fees as a result of Defendants' violations of the Illinois CFA.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all other similarly situated, pray for relief as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiffs as representatives of the Classes and Plaintiffs' attorneys as Class Counsel to represent the Classes;

B. For an order finding in favor of Plaintiffs and the Class on all causes of action asserted herein;

C. For compensatory, statutory, and/or punitive damages in amounts to be determined by the trier of fact;

D. For an order of restitution and all other forms of equitable monetary relief;

E. Declaratory and injunctive relief as described herein;

F. Awarding Plaintiffs' reasonable attorneys' fees, costs, and expenses;

G. Awarding pre- and post-judgment interest on any amounts awarded; and

H. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: August 16, 2024

Respectfully Submitted,

/s/ Kenneth J. Grunfeld

KENNETH J. GRUNFELD, ESQUIRE
New Jersey Bar No. 026091999
JEFF OSTROW, ESQUIRE*
KOPELOWITZ OSTROW
FERGUSON WEISELBERG GILBERT
65 Overhill Road
Bala Cynwyd, PA 19004
Tel.: (954) 525-4100
grunfeld@kolawyers.com
ostrow@kolawyers.com

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

(**pro hac vice application forthcoming)*

Attorneys for the Plaintiffs and Putative Class

ClassAction.org
